CISCO SYSTEMS

# Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide

Product and Documentation Release 3.4
Last Updated: August 109, 2005

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

*Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 3.4*

# CONTENTS

**Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4**

**Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4**

**FIGURES**

**T A B L E S**

# Preface

This section explains who should read the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4,* how the document is organized, related documentation, document conventions, how to order print and CD-ROM documentation, and how to obtain technical assistance.

# Audience

This guide is for Cisco ONS 15454 SDH users who are responsible for troubleshooting and maintenance. General troubleshooting categories and a comprehensive list of ONS 15454 SDH alarms are provided. These sections include procedures for correcting every troubleshooting issue. All maintenance procedures are included, as well as detailed card reference information.

Users responsible for installing and configuring ONS 15454 SDH nodes should have the companion *Cisco ONS 15454 SDH Installation and Operations Guide*.

# Organization

| Chapter and Title | Description |
|---|---|
| Chapter 1, "Alarm Troubleshooting" | Alphabetically lists the alarms generated by the ONS 15454 SDH and provides troubleshooting procedures for each alarm. |
| Chapter 2, "General Troubleshooting" | Explains several common troubleshooting topics and provides their solution procedures. |
| Chapter 3, "Card Reference" | Provides a functional description, illustration, block diagram, and specifications for every ONS 15454 SDH FMEC and card. |
| Chapter 4, "Maintenance" | Explains how to perform several routine hardware and software maintenance procedures. |
| Glossary | Defines commonly-used terms. |

# Related Documentation

The following documentation can be used in conjunction with this manual:

- *Cisco ONS 15454 SDH Installation and Operations Guide, Release 3.4*
- *Cisco ONS 15454 SDH Product Overview, Release 3.4*
- *Release Notes for the Cisco ONS 15454 SDH, Release 3.4*
- *Cisco Warranty Services for ONG Products*
- *Installing the Cisco ONS 15454 SDH Conducted Emissions Kit* (Required for EMEA compliance only)

# Conventions

The following conventions are used throughout this publication:

**Note**     Means reader take note. Notes contain helpful suggestions or useful background information.

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

**Warning**     **Means reader be careful. In this situation, you might do something that could result in harm to yourself or others.**

**Tip**     Means the information might help you solve a problem.

| Convention | Definition |
|---|---|
| **Bold** text | Denotes icons, buttons, or tabs that the user must select. |
| > | Used to separate consecutive actions; for example, "click the Maintenance > Protection > Ring tabs." |
| **Procedure:** | Precedes all procedures; a horizontal line indicates the end of each procedure. |

# Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

# World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

# Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

# Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

# Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

**C H A P T E R 1**

# Alarm Troubleshooting

This chapter gives a list of alarm descriptions, default severities, and troubleshooting procedures for all alarms that can be resolved in the Cisco ONS 15454 SDH system. See Table 1-1 on page 1-1 for an alphabetical list of alarms that appear on the ONS 15454 SDH. See Table 1-6 on page 1-5 for a list of alarms organized by alarm type. This chapter provides comprehensive lists of alarm conditions with severities of Critical, Major, or Minor.

All listed alarm severities are defaults for active cards, if applicable. Active cards have provisioned ports, even if they are not put in service. Cards with unprovisioned ports are considered inactive. The default severity for all inactive card alarms is Minor, Non-Service-Affecting. The default standby severity for conditions with a severity of Not Alarmed (NA), Non-Service Affecting is NA, NSA. The default standby severity for conditions with a severity of Not Reported (NR), NSA is NR, NSA. Alarm severities can be changed by single alarm or by profile. For more information about this, see the Alarm Monitoring and Management Chapter in the *Cisco ONS 15454 SDH Installation and Operations Guide*. The troubleshooting procedures in this chapter apply to the Cisco Transport Controller (CTC) version of that alarm.

Log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco Technical Assistance Center (TAC) toll-free numbers for your country to obtain more information.

## 1.1 Alarm Index by Default Severity

The alarm index by default severity groups alarms and conditions by the severity displayed in the CTC Alarms tab in the severity (SEV) column.

### 1.1.1 Critical Alarms (CR)

Table 1-1 lists of critical alarms.

*Table 1-1 Critical Alarm Index*

| AU-LOP, page 1-20 | EQPT-MISS, page 1-44 | MEA (Bplane), page 1-75 |
|---|---|---|
| AUTOLSROFF, page 1-21 | FAN, page 1-53 | MEA (EQPT), page 1-76 |
| BKUPMEMP, page 1-25 | HITEMP, page 1-59 | MEA (FAN), page 1-77 |
| COMIOXC, page 1-32 | HP-UNEQ, page 1-62 | MFGMEM, page 1-79 |

*Table 1-1    Critical Alarm Index (continued)*

| | | |
|---|---|---|
| CTNEQPT-PBPROT, page 1-37 | IMPROPRMVL, page 1-62 | MFGMEM (Backplane or Fan), page 1-80 |
| CTNEQPT-PBWORK, page 1-38 | LP-UNEQ, page 1-73 | SWMTXMOD, page 1-97 |
| EQPT, page 1-44 | | |

# 1.1.2  Major Alarms (MJ)

Table 1-2 lists major alarms.

*Table 1-2    Major Alarm Index*

| | | |
|---|---|---|
| APSCM, page 1-17 | ELWBATVG-B, page 1-41 | LOS (DS-3, E-N, STM-N), page 1-69 |
| APSCNMIS, page 1-17 | EOC, page 1-42 | MEM-GONE, page 1-78 |
| CARLOSS (E-Series), page 1-27 | E-W-MISMATCH, page 1-45 | MSSP-OOSYNC, page 1-82 |
| CARLOSS (G1000-4), page 1-29 | EXTRA-TRAF-PREEMPT, page 1-48 | PRC-DUPID, page 1-83 |
| CONTBUS-A-18, page 1-33 | FRNGSYNC, page 1-58 | PWR-A, page 1-84 |
| CONTBUS-B-18, page 1-34 | HLDOVRSYNC, page 1-60 | PWR-B, page 1-85 |
| CONTBUS-IO-A, page 1-34 | INVMACADR, page 1-65 | RING-MISMATCH, page 1-85 |
| CONTBUS-IO-B, page 1-36 | LOF (BITS), page 1-67 | SYSBOOT, page 1-102 |
| EHIBATVG-A, page 1-40 | LOF (DS3, E-N, STM-N), page 1-68 | TPTFAIL, page 1-102 |
| EHIBATVG-B, page 1-41 | LOS (BITS), page 1-69 | TRMT, page 1-103 |
| ELWBATVG-A, page 1-41 | | |

# 1.1.3  Minor Alarms (MN)

Table 1-3 lists minor alarms.

*Table 1-3    Minor Alarm Index*

| | | |
|---|---|---|
| APSB, page 1-14 | EXCCOL, page 1-47 | PROTNA, page 1-83 |
| APSCDFLTK, page 1-15 | EXT, page 1-48 | SFTWDOWN, page 1-90 |
| APSC-IMP, page 1-16 | FEPRLF, page 1-57 | SNTP-HOST, page 1-91 |
| APSCINCON, page 1-16 | FSTSYNC, page 1-59 | SSM-FAIL (BITS), page 1-93 |
| AUTORESET, page 1-22 | HP-TIM, page 1-61 | SSM-FAIL (STM-N), page 1-93 |
| AUTOSW-LOP-SNCP, page 1-23 | LP-PLM, page 1-72 | SYNCPRI, page 1-100 |
| AUTOSW-UNEQ-SNCP, page 1-24 | MEM-LOW, page 1-78 | SYNCSEC, page 1-100 |
| CARLOSS (EQPT), page 1-26 | NOT-AUTHENTICATED, page 1-83 | SYNCTHIRD, page 1-101 |
| DATAFLT, page 1-40 | | |

## 1.1.4 Conditions (NA or NR)

Table 1-4 lists conditions that are not alarmed or not reported.

*Table 1-4*    *Conditions Index*

| | | |
|---|---|---|
| AIS, page 1-14 | FULLPASSTHR-BI, page 1-59 | RING-SW-WEST, page 1-86 |
| AS-CMD, page 1-18 | HP-RFI, page 1-61 | SD, page 1-86 |
| AS-MT, page 1-19 | INHSWPR, page 1-64 | SDBER-EXCEED-HO, page 1-88 |
| AU-AIS, page 1-19 | INHSWWKG, page 1-64 | SF, page 1-88 |
| AUTOSW-AIS-SNCP, page 1-22 | KB-PASSTHR, page 1-65 | SFBER-EXCEED-HO, page 1-90 |
| AUTOSW-SDBER-SNCP, page 1-24 | LKOUTPR-S, page 1-65 | SPAN-SW-EAST, page 1-91 |
| AUTOSW-SFBER-SNCP, page 1-24 | LKOUTWK-R, page 1-66 | SPAN-SW-WEST, page 1-91 |
| CLDRESTART, page 1-31 | LKOUTWK-S, page 1-66 | SQUELCH, page 1-92 |
| E3-ISD, page 1-40 | LOCKOUT-REQ, page 1-66 | SSM-DUS, page 1-93 |
| EXERCISE-RING-REQ, page 1-47 | LOCKOUT-REQ-SPAN, page 1-67 | SSM-LNC, page 1-94 |
| EXERCISE-SPAN-REQ, page 1-48 | LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 | SSM-OFF (BITS), page 1-94 |
| FAILTOSW, page 1-49 | LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 | SSM-OFF (STM-N), page 1-94 |
| FAILTOSW-HO, page 1-49 | LPBKTERMINAL(G1000-4), page 1-71 | SSM-PRC, page 1-95 |
| FAILTOSW-LO, page 1-50 | LP-RFI, page 1-72 | SSM-SETS, page 1-95 |
| FAILTOSWR, page 1-51 | MAN-REQ, page 1-73 | SSM-STU (BITS), page 1-95 |
| FAILTOSWS, page 1-53 | MANRESET, page 1-73 | SSM-STU (STM-N), page 1-96 |
| FE-EXERCISING-RING, page 1-54 | MANSWTOINT, page 1-74 | SSM-TNC (BITS), page 1-96 |
| FE-EXERCISING-SPAN, page 1-54 | MANSWTOPRI, page 1-74 | SWTOPRI, page 1-98 |
| FE-FRCDWKSWPR-RING, page 1-54 | MANSWTOSEC, page 1-74 | SWTOSEC, page 1-98 |
| FE-FRCDWKSWPR-SPAN, page 1-55 | MANSWTOTHIRD, page 1-74 | SWTOTHIRD, page 1-99 |
| FE-LOCKOUTOFPR-SPAN, page 1-55 | MANUAL-REQ-RING, page 1-74 | SYNC-FREQ (BITS, STM-N), page 1-99 |
| FE-MANWKSWPR-RING, page 1-56 | MANUAL-REQ-SPAN, page 1-75 | TU-AIS, page 1-103 |
| FE-MANWKSWPR-SPAN, page 1-56 | MS-AIS, page 1-81 | TU-LOP, page 1-104 |
| FORCED-REQ, page 1-57 | MS-RFI, page 1-81 | WKSWPR, page 1-104 |
| FORCED-REQ-RING, page 1-58 | RAI, page 1-85 | WTR, page 1-105 |
| FORCED-REQ-SPAN, page 1-58 | RING-SW-EAST, page 1-86 | |

# 1.2 Alarm Index Alphabetical

Table 1-5 lists alarms by the name displayed on the CTC Alarms tab in the conditions column.

*Table 1-5    Alarm Index*

*Table 1-5     Alarm Index (continued)*

| | | |
|---|---|---|
| ELWBATVG-A, page 1-41 | LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 | SSM-STU (STM-N), page 1-96 |
| ELWBATVG-B, page 1-41 | LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 | SSM-TNC (BITS), page 1-96 |
| EOC, page 1-42 | LPBKTERMINAL(G1000-4), page 1-71 | SSM-TNC (STM-N), page 1-97 |
| EQPT, page 1-44 | LP-PLM, page 1-72 | SWMTXMOD, page 1-97 |
| EQPT-MISS, page 1-44 | LP-RFI, page 1-72 | SWTOPRI, page 1-98 |
| E-W-MISMATCH, page 1-45 | LP-UNEQ, page 1-73 | SWTOSEC, page 1-98 |
| EXCCOL, page 1-47 | MAN-REQ, page 1-73 | SWTOTHIRD, page 1-99 |
| EXERCISE-RING-REQ, page 1-47 | MANRESET, page 1-73 | SYNC-FREQ (BITS, STM-N), page 1-99 |
| EXERCISE-SPAN-REQ, page 1-48 | MANSWTOINT, page 1-74 | SYNCTHIRD, page 1-101 |
| EXT, page 1-48 | MANSWTOPRI, page 1-74 | SYSBOOT, page 1-102 |
| EXTRA-TRAF-PREEMPT, page 1-48 | MANSWTOSEC, page 1-74 | TPTFAIL, page 1-102 |
| FAILTOSW, page 1-49 | MANSWTOTHIRD, page 1-74 | TRMT, page 1-103 |
| FAILTOSW-HO, page 1-49 | MANUAL-REQ-RING, page 1-74 | TU-AIS, page 1-103 |
| FAILTOSW-LO, page 1-50 | MANUAL-REQ-SPAN, page 1-75 | TU-LOP, page 1-104 |
| FAILTOSWR, page 1-51 | MEA (Bplane), page 1-75 | WKSWPR, page 1-104 |
| FAILTOSWS, page 1-53 | MEA (EQPT), page 1-76 | WTR, page 1-105 |
| FAN, page 1-53 | MEA (FAN), page 1-77 | |

# 1.3  Alarm Index by Alarm Type

Table 1-6 gives the name and page number of every alarm in the chapter organized by alarm type.

*Table 1-6     Alarm Index by Alarm Type*

| |
|---|
| AIP: EQPT, page 1-44 |
| AIE: EQPT, page 1-44 |
| AIE: MFGMEM (Backplane or Fan), page 1-80 |
| BITS: AIS, page 1-14 |
| BITS: LOF (BITS), page 1-67 |
| BITS: LOS (BITS), page 1-69 |
| BITS: SSM-DUS, page 1-93 |
| BITS: SSM-FAIL (BITS), page 1-93 |
| BITS: SSM-LNC, page 1-94 |
| BITS: SSM-OFF (BITS), page 1-94 |
| BITS: SSM-PRC, page 1-95 |

*Table 1-6     Alarm Index by Alarm Type (continued)*

| |
|---|
| BITS: SSM-SETS, page 1-95 |
| BITS: SSM-STU (BITS), page 1-95 |
| BITS: SSM-TNC (BITS), page 1-96 |
| BITS: SYNC-FREQ (BITS, STM-N), page 1-99 |
| BPLANE: AS-CMD, page 1-18 |
| BPLANE: INVMACADR, page 1-65 |
| BPLANE: MEA (Bplane), page 1-75 |
| BPLANE: MFGMEM (Backplane or Fan), page 1-80 |
| DS3: AIS, page 1-14 |
| DS3: AS-CMD, page 1-18 |
| DS3: AS-MT, page 1-19 |
| DS3: LOF (DS3, E-N, STM-N), page 1-68 |
| DS3: LOS (DS-3, E-N, STM-N), page 1-69 |
| DS3: LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 |
| DS3: RAI, page 1-85 |
| E-1: AS-CMD, page 1-18 |
| E-1: AIS, page 1-14 |
| E-1: AS-MT, page 1-19 |
| E-1: LOF (DS3, E-N, STM-N), page 1-68 |
| E-1: LOF (DS3, E-N, STM-N), page 1-68 |
| E-1: LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 |
| E-1: LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 |
| E-1: RAI, page 1-85 |
| E-1: TRMT, page 1-103 |
| E-3: AIS, page 1-14 |
| E-3: AS-CMD, page 1-18 |
| E-3: AS-MT, page 1-19 |
| E-3: E3-ISD, page 1-40 |
| E-3: LOS (DS-3, E-N, STM-N), page 1-69 |
| E-3: LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 |
| E-3: LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 |
| EC-N: AS-CMD, page 1-18 |
| EC-N: AS-MT, page 1-19 |
| EC-N: LOF (DS3, E-N, STM-N), page 1-68 |
| EC-N: LOS (DS-3, E-N, STM-N), page 1-69 |
| EC-N: LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 |
| EC-N: LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 |

***Table 1-6    Alarm Index by Alarm Type (continued)***

*Table 1-6    Alarm Index by Alarm Type (continued)*

| |
|---|
| EXTSYNC: SWTOSEC, page 1-98 |
| EXTSYNC: SWTOTHIRD, page 1-99 |
| EXTSYNC: SYNCPRI, page 1-100 |
| EXTSYNC: SYNCSEC, page 1-100 |
| EXTSYNC: SYNCTHIRD, page 1-101 |
| FAN: EQPT-MISS, page 1-44 |
| FAN: FAN, page 1-53 |
| FAN: MEA (FAN), page 1-77 |
| FAN: MFGMEM (Backplane or Fan), page 1-80 |
| FUDC: AIS, page 1-14 |
| FUDC: LOF (DS3, E-N, STM-N), page 1-68 |
| HDGE [G1000]: CARLOSS (G1000-4), page 1-29 |
| HDGE [G1000]: LPBKTERMINAL(G1000-4), page 1-71 |
| HDGE [G1000]: TPTFAIL, page 1-102 |
| HPMON: AU-AIS, page 1-19 |
| HPMON: AU-LOP, page 1-20 |
| HPMON: AUTOSW-AIS-SNCP, page 1-22 |
| HPMON: AUTOSW-LOP-SNCP, page 1-23 |
| HPMON: AUTOSW-SDBER-SNCP, page 1-24 |
| HPMON: AUTOSW-SFBER-SNCP, page 1-24 |
| HPMON: AUTOSW-UNEQ-SNCP, page 1-24 |
| HPMON: FAILTOSW-HO, page 1-49 |
| HPMON: FORCED-REQ, page 1-57 |
| HPMON: HP-RFI, page 1-61 |
| HPMON: HP-TIM, page 1-61 |
| HPMON: HP-UNEQ, page 1-62 |
| HPMON: LOCKOUT-REQ, page 1-66 |
| HPMON: MAN-REQ, page 1-73 |
| HPMON: SDBER-EXCEED-HO, page 1-88 |
| HPMON: SFBER-EXCEED-HO, page 1-90 |
| HPMON: WKSWPR, page 1-104 |
| HPTERM:AU-AIS, page 1-19 |
| HPTERM:AU-LOP, page 1-20 |
| HPTERM:HP-TIM, page 1-61 |
| HPTERM:HP-UNEQ, page 1-62 |
| HPTERM:SDBER-EXCEED-HO, page 1-88 |
| HPTERM:SFBER-EXCEED-HO, page 1-90 |

*Table 1-6    Alarm Index by Alarm Type (continued)*

| |
| --- |
| LPMON:AUTOSW-AIS-SNCP, page 1-22 |
| LPMON: AUTOSW-LOP-SNCP, page 1-23 |
| LPMON: AUTOSW-SDBER-SNCP, page 1-24 |
| LPMON: AUTOSW-SFBER-SNCP, page 1-24 |
| LPMON: AUTOSW-SFBER-SNCP, page 1-24 |
| LPMON: FAILTOSW-LO, page 1-50 |
| LPMON: FORCED-REQ, page 1-57 |
| LPMON: LOCKOUT-REQ, page 1-66 |
| LPMON: LP-UNEQ, page 1-73 |
| LPMON: MAN-REQ, page 1-73 |
| LPMON: TU-AIS, page 1-103 |
| LPMON: TU-LOP, page 1-104 |
| LPMON: WKSWPR, page 1-104 |
| LPTERM: LP-PLM, page 1-72 |
| LPTERM: LP-RFI, page 1-72 |
| LPTERM: LP-UNEQ, page 1-73 |
| LPTERM: SD, page 1-86 |
| LPTERM: SF, page 1-88 |
| LPTERM: TU-AIS, page 1-103 |
| LPTERM: TU-LOP, page 1-104 |
| NE: DATAFLT, page 1-40 |
| NE: EHIBATVG-A, page 1-40 |
| NE: EHIBATVG-B, page 1-41 |
| NE: ELWBATVG-A, page 1-41 |
| NE: EHIBATVG-B, page 1-41 |
| NE: PRC-DUPID, page 1-83 |
| NE: PWR-A, page 1-84 |
| NE: PWR-B, page 1-85 |
| NE: SNTP-HOST, page 1-91 |
| NE: SYSBOOT, page 1-102 |
| NERING: FULLPASSTHR-BI, page 1-59 |
| NERING: MSSP-OOSYNC, page 1-82 |
| NERING: PRC-DUPID, page 1-83 |
| NERING: RING-MISMATCH, page 1-85 |
| NESYNC: FRNGSYNC, page 1-58 |
| NESYNC: FSTSYNC, page 1-59 |
| NESYNC: HLDOVRSYNC, page 1-60 |

*Table 1-6*     *Alarm Index by Alarm Type (continued)*

| |
| --- |
| NESYNC: KB-PASSTHR, page 1-65 |
| NESYNC: MANSWTOINT, page 1-74 |
| NESYNC: MANSWTOPRI, page 1-74 |
| NESYNC: MANSWTOSEC, page 1-74 |
| NESYNC: MANSWTOTHIRD, page 1-74 |
| NESYNC: SSM-SETS, page 1-95 |
| NESYNC: SSM-STU (STM-N), page 1-96 |
| NESYNC: SSM-TNC (STM-N), page 1-97 |
| NESYNC: SWTOPRI, page 1-98 |
| NESYNC: SWTOSEC, page 1-98 |
| NESYNC: SWTOTHIRD, page 1-99 |
| NESYNC: SYNCPRI, page 1-100 |
| NESYNC: SYNCSEC, page 1-100 |
| NESYNC: SYNCTHIRD, page 1-101 |
| NE: EQPT, page 1-44 |
| STM-N: APSB, page 1-14 |
| STM-N: APSB, page 1-14 |
| STM-N: APSCDFLTK, page 1-15 |
| STM-N: APSC-IMP, page 1-16 |
| STM-N: APSCINCON, page 1-16 |
| STM-N: APSCM, page 1-17 |
| STM-N: AS-CMD, page 1-18 |
| STM-N: AS-MT, page 1-19 |
| STM-N: AUTOLSROFF, page 1-21 |
| STM-N: EOC, page 1-42 |
| STM-N: E-W-MISMATCH, page 1-45 |
| STM-N: EXERCISE-RING-REQ, page 1-47 |
| STM-N: EXERCISE-SPAN-REQ, page 1-48 |
| STM-N: EXTRA-TRAF-PREEMPT, page 1-48 |
| STM-N: FAILTOSW, page 1-49 |
| STM-N: FAILTOSWR, page 1-51 |
| STM-N: FAILTOSWS, page 1-53 |
| STM-N: FE-EXERCISING-RING, page 1-54 |
| STM-N: FE-EXERCISING-SPAN, page 1-54 |
| STM-N: FE-FRCDWKSWPR-RING, page 1-54 |
| STM-N: FE-FRCDWKSWPR-SPAN, page 1-55 |
| STM-N: FE-LOCKOUTOFPR-SPAN, page 1-55 |

*Table 1-6    Alarm Index by Alarm Type (continued)*

| |
|---|
| STM-N: FE-MANWKSWPR-RING, page 1-56 |
| STM-N: FE-MANWKSWPR-SPAN, page 1-56 |
| STM-N: FEPRLF, page 1-57 |
| STM-N: FORCED-REQ-RING, page 1-58 |
| STM-N: FORCED-REQ-SPAN, page 1-58 |
| STM-N: LKOUTPR-S, page 1-65 |
| STM-N: LKOUTWK-R, page 1-66 |
| STM-N: LKOUTWK-S, page 1-66 |
| STM-N: LOCKOUT-REQ, page 1-66 |
| STM-N: LOCKOUT-REQ-RING, page 1-66 |
| STM-N: LOF (DS3, E-N, STM-N), page 1-68 |
| STM-N: LOS (DS-3, E-N, STM-N), page 1-69 |
| STM-N: LPBKFACILITY (DS-3, E-N, STM-N), page 1-70 |
| STM-N: LPBKTERMINAL (DS-3, E-N, STM-N), page 1-71 |
| STM-N: MANUAL-REQ-RING, page 1-74 |
| STM-N: MANUAL-REQ-SPAN, page 1-75 |
| STM-N: MS-AIS, page 1-81 |
| STM-N: MS-RFI, page 1-81 |
| STM-N: RING-SW-EAST, page 1-86 |
| STM-N: RING-SW-WEST, page 1-86 |
| STM-N: SD, page 1-86 |
| STM-N: SF, page 1-88 |
| STM-N: SPAN-SW-EAST, page 1-91 |
| STM-N: SPAN-SW-WEST, page 1-91 |
| STM-N: SQUELCH, page 1-92 |
| STM-N: SSM-DUS, page 1-93 |
| STM-N: SSM-FAIL (STM-N), page 1-93 |
| STM-N: SSM-LNC, page 1-94 |
| STM-N: SSM-OFF (STM-N), page 1-94 |
| STM-N: SSM-PRC, page 1-95 |
| STM-N: SSM-SETS, page 1-95 |
| STM-N: SSM-STU (STM-N), page 1-96 |
| STM-N: SSM-TNC (STM-N), page 1-97 |
| STM-N: SYNC-FREQ (BITS, STM-N), page 1-99 |
| STM-N: WKSWPR, page 1-104 |
| STM-N: WTR, page 1-105 |

## 1.3.1 Alarm Type/Object Definition

Table 1-7 defines abbreviations used in the alarm troubleshooting procedures.

*Table 1-7    Alarm Type/Object Definition*

| | |
|---|---|
| **BITS** | Building integration timing supply (BITS) incoming references (BITS-1, BITS-2) |
| **BPLANE** | Backplane |
| **E1** | E1-N-14 card |
| **E3** | E3-12 card |
| **E-N** | E-1 or E-3 |
| **EQPT** | A card in any of the 17 card slots. This object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, and VC. |
| **ETHER** | Ethernet |
| **FAN** | Fan-tray assembly |
| **NE** | The entire network element (SYSTEM) |
| **NERINGSDH** | SDH NE[1] ring |
| **NESYNCHSDH** | SDH NE synchronization |
| **STMN** | Synchronous Transfer Mode (speed) |

1. Network element

# 1.4 Trouble Notifications

The ONS 15454 SDH uses ITU-T x.733-compliant categories to characterize alarm levels. In CTC, the Critical, Major, and Minor ONS 15454 SDH alarms are reported in the Alarms tab. This tab contains alarms such as loss of signal (LOS) indicating problems a user must correct. The ONS CTC Conditions tab contains ONS 15454 SDH conditions as well as alarms. If a condition is not listed in the Alarms tab as well, it is a notification and does not require user action.

Alarms are further divided into Service Affecting (SA) and NSA status. An SA failure affects a provided service or the network's ability to provide service. The high temperature (HITEMP) alarm, which means the ONS 15454 SDH is hotter than 50 degrees Celsius (122 degrees Fahrenheit), is an SA failure. For example, although a particular E-1 port might not be affected, a high temperature affects the network's ability to provide service.

## 1.4.1 Conditions

When an SA failure is detected, the ONS 15454 SDH also sends an alarm indication signal (AIS) downstream. When it receives the AIS, the receiving node sends a remote failure indication (RFI) upstream. AIS and RFI belong in the conditions category and are shown on the Conditions tab of the ONS 15454 SDH. The condition reporting is not ITU-compliant.

## 1.4.2 Severities

The ONS 15454 SDH uses these ITU severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service-affecting alarm that needs immediate correction. Major is still a serious alarm, but the failure has less of an impact on the network.

Minor alarms, such as Fast Start Synchronization (FSTSYNC), do not have a serious effect on service. FSTSYNC lets you know that the ONS 15454 SDH is choosing a new timing reference because the old reference failed. The loss of the prior timing source is something a user needs to troubleshoot, but this minor alarm should not disrupt service.

The ONS 15454 SDH uses standard severity reporting that is ITU-compliant. You can customize ONS 15454 SDH alarm severities with the alarm profiles feature. For additional information about alarm severities, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

# 1.5  Safety Summary

This section covers safety considerations to ensure safe operation of the ONS 15454 SDH system. Personnel should not perform any procedures in this manual unless they understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards. In these instances, users should pay close attention to the following caution.

**Caution**    Hazardous voltage or energy might be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of optical (STM) cards. In these instances, users should pay close attention to the following warnings.

**Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Warning**    **Class 1 laser product.**

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

# 1.6 Alarm Procedures

This section lists alarms alphabetically. Each alarm or condition topic gives the severity, description, and troubleshooting procedure.

## 1.6.1 AIS

- Not Reported (NR) (Condition)

The ONS 15454 SDH detects an Alarm Indication Signal (AIS) in the SDH overhead. This condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but the DS-3 or STM-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service or has an out-of-service port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

### Procedure: Clear the AIS Condition

**Step 1**    Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports.

**Step 2**    If the condition does not clear, clear the upstream alarms using the applicable procedure(s) in this chapter.

**Step 3**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.2 APSB

- Minor (MN), Non-Service Affecting (NSA)

The Channel Byte Failure alarm occurs when line terminating equipment detects protection switching byte failure in the incoming automatic protection switching (APS) signal. This happens when an inconsistent APS byte or invalid code is detected. Some older, non-Cisco SDH nodes send invalid APS codes if configured in a 1+1 protection scheme with newer SDH nodes, such as the ONS 15454 SDH. These invalid codes raise an APSB on an ONS 15454 SDH node.

### Procedure: Clear the APSB Alarm

**Step 1**    Examine the incoming SDH overhead with an optical test set to confirm inconsistent or invalid K bytes.

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

**Step 2**    If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454 SDH. You might need to replace the upstream cards for protection switching to operate properly.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.3  APSCDFLTK

- Minor (MN), Non-Service Affecting (NSA)

The Default K Byte received alarm occurs when an multiplex section-shared protection ring (MS-SPRing) is not properly configured. For example, it occurs when a four-node MS-SPRing has one node configured as an SNCP ring. In this case, a node in an subnetwork connection protection (SNCP) or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for MS-SPRing. One of the bytes sent is considered invalid by the MS-SPRing configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

**Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

**Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the APSCDFLTK Alarm

**Step 1**    Verify that each node has a unique node ID number by using the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 2**    Repeat Step 1 for all nodes in the ring.

If two nodes have the same node ID number, use the "Change a Node ID Number" procedure on page 1-106 to change one node's ID number so that each node ID is unique.

**Step 3**    If the alarm does not clear, verify correct configuration of east port and west port optical fibers (see the "E-W-MISMATCH" section on page 1-45). West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 SDH Installation and Operations Guide* provides a procedure for fibering MS-SPRings.

**Step 4**    If the alarm does not clear and if it is a four-fiber MS-SPRing system, make sure 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 protection fiber.

**Step 5**    If the alarm does not clear, check the ring in network view and verify that each node is visible to the other nodes using the "Verify Node Visibility for Other Nodes" procedure on page 1-106.

**Step 6**    If nodes are not visible, use the "Check or Create Node SDCC Terminations" procedure on page 1-106 to ensure that SDCC terminations exist on each node.

**Step 7**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.4 APSC-IMP

- Minor (MN), Non-Service Affecting (NSA)

An Improper APS Code alarm indicates invalid K bytes. This alarm occurs on STM-N cards in an MS-SPRing configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. APSC-IMP occurs when these bits indicate a bad or invalid K byte. The alarm clears when the node receives valid K bytes.

⚠️

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: 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.

If the K byte is invalid, the problem lies in upstream equipment and not in the reporting ONS 15454 SDH. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454 SDHs, consult the appropriate user documentation.

**Step 2**    If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs. Use the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 3**    Repeat Step 2 for all nodes in the ring.

**Step 4**    If a node has a ring ID number that does not match the other nodes, make the ring ID number of that node identical to the other nodes. Use the "Change a Ring ID Number" procedure on page 1-105.

**Step 5**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.5 APSCINCON

- Minor (MN), Service Affecting (SA)

An Inconsistent APS Code alarm indicates that the APS code contained in the SDH overhead is inconsistent. The SDH overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454 SDH, to switch the SDH signal from a working to a protect path. An inconsistent APS code occurs when three consecutive frames do not contain identical APS bytes. Inconsistent APS bytes give the receiving equipment conflicting commands about switching.

## Procedure: Clear the APSCINCON Alarm on an STM-N Card in an MS-SPRing

**Step 1**    Look for other alarms, especially LOS (DS-3, E-N, STM-N), loss of frame (LOF (DS3, E-N, STM-N)) or AIS. Clearing these alarms clears the APSCINCON alarm.

**Step 2**    If an APSINCON alarm occurs with no other alarms, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.6  APSCM

- Major (MJ), Service Affecting (SA)

The APS Channel Mismatch alarm occurs when the ONS 15454 SDH expects a working channel but receives a protection channel. In many cases, the working and protection channels are crossed and the protection channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. This alarm is raised in a 1+1 configuration. The APSCM alarm only occurs on the ONS 15454 SDH when 1+1 bidirectional protection is used on STM-N cards in a 1+1 configuration.

**Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

### Procedure: Clear the APSCM Alarm

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

**Step 2**    If the alarm does not clear, verify that the protection-card channel fibers are physically connected directly to the adjoining node's protection-card channel fibers.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.7  APSCNMIS

- Major (MJ), Service Affecting (SA)

The Node ID Mismatch alarm raises when the source node ID contained in the K2 byte of the APS channel being received is not present in the ring map. This alarm might occur and clear when an MS-SPRing is being provisioned. If so, the user can disregard the temporary occurrence. If the APSCNMIS is raised and stays, the alarm clears when a K byte with a valid source node ID is received.

## Procedure: Clear the APSCNMIS Alarm

**Step 1**   Verify that each node has a unique node ID number using the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 2**   If the Nodes column contains any two nodes with the same node ID listed, record the repeated node ID.

**Step 3**   Click **Close** on the Ring Map dialog box.

**Step 4**   If two nodes have the same node ID number, use the "Change a Node ID Number" procedure on page 1-106 to change one node's ID number so that each node ID is unique.

> ✎
>
> **Note**   If the node names shown on the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. This window displays the node ID of the node you are logged into.

> ✎
>
> **Note**   Locking out and clearing the lockout on a span causes the ONS 15454 SDH 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, lock out the span using the "Lock Out an MS-SPRing Span" procedure on page 1-107.

**Step 6**   Clear the lockout using the "Clear an MS-SPRing Span Command" procedure on page 1-107.

**Step 7**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.8  AS-CMD

- Not Alarmed (NA) (Condition)

The Alarms Suppressed by User Command condition applies to the node, backplane, and cards. This condition is caused when alarms are suppressed for one or more cards or for the entire shelf.

## Procedure: Clear the AS-CMD Condition

**Step 1**   Click the **Conditions** tab. From the Object column and Eqpt Type column, note what entity the condition is reported against, such as against a port, slot, shelf, or against the ONS 15454 SDH.

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 go to Step 2.

If the condition is reported against the backplane, go to Step 6.

If the **Condition** tab says that the object is "system," it means that it applies to the shelf. Go to Step 7.

**Step 2**    If the AS-CMD condition is reported for a card, determine whether alarms are suppressed for a port and if so, raise the suppressed alarms.

    **a.**    Double-click the card to display the card view.

    **b.**    Click the **Provisioning > Alarm Behavior** tabs.

        –   If the Suppress Alarms column check box is checked for a port row, click it to 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 Parent View**.

**Step 3**    In the CTC node (default login) view, if the AS-CMD condition is reported for a card and not an individual port, click the **Provisioning > Alarm Behavior** tabs.

**Step 4**    Locate the row for the reported card slot. (The slot number information was in the Object column in the **Conditions** tab that you noted in Step 1.)

**Step 5**    Click the **Suppress Alarms** column check box to deselect the option for the card row.

**Step 6**    If the condition is reported for the backplane, the alarms are suppressed for cards such as the alarm interface panel (AIP) that are not in the optical or electrical slots.

    **a.**    In the CTC node (default login) view, click the **Provisioning > Alarm Behavior** tabs.

    **b.**    In the Backplane row, click the **Suppress Alarms** column check box to deselect it and click **Apply**.

**Step 7**    If the condition is reported for the shelf, then cards and other equipment are affected.

    **a.**    In the CTC node (default login) view, click the **Provisioning > Alarm Behavior** tabs.

    **b.**    Click the **Suppress Alarms** check box located at the bottom of the tab to deselect the option.

    **c.**    Click **Apply**.

**Step 8**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.9 AS-MT

•   Not Alarmed (NA) (Condition)

The Alarms Suppressed for Maintenance Command condition applies to optical and electrical cards and is raised when a port is placed in out of service (OOS) maintenance (OOS-MT) state for loopback testing operations.

To clear the AS-MT condition by clearing the loopback, follow the "Clear a Loopback" procedure on page 1-108. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.10 AU-AIS

•   Not Reported (NR) (Condition)

An Administration Unit (AU) AIS condition applies to the administration unit, which consists of the virtual container (VC) capacity and pointer bytes (H1, H2, and H3) in the SDH frame. This condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but the DS-3 or STM-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service, loss of frame, bit error signal degrade or failure, trace identifier mismatch, or an out-of-service port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

## Procedure: Clear the AU-AIS Condition

**Step 1**    Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports.

**Step 2**    Clear the upstream alarms using the applicable procedure(s) in this chapter.

**Step 3**    If the condition does not clear, follow the procedure in the "APSB" section on page 1-14.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.11  AU-LOP

- Critical (CR), Service Affecting (SA)

An Administration Unit Loss of Pointer (LOP) alarm applies to the administration unit, which consists of the VC capacity and pointer bytes (H1, H2, and H3) in the SDH frame. This alarm is caused when the first payload pointer is not synchronized according to the system clock.

**Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

**Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the AU-LOP Alarm

**Step 1**    Check for LOS (DS-3, E-N, STM-N) on the reporting card and clear that alarm if applicable.

**Step 2**    If the AU-LOP does not clear, check whether attenuation is present on the input fiber cable on the card raising the alarm.

**Step 3**    If the alarm does not clear, check the signal level on the input fiber with the attenuator (if present).

**Step 4**    If the fiber signal level with an attenuator is below the correct threshold, remove the attenuator and check signal level again.

**Step 5**    If the signal level is still low, clean both ends of the fiber cable connection according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 6** If the alarm does not clear, clean the far-end optical fiber cable ends.

**Step 7** If error remains, check for a timing alarm. Follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 8** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.12  AUTOLSROFF

- Critical (CR), Service Affecting (SA)

The Automatic Laser Off alarm is raised when the OC192 LR/STM64 LH 1550 card temperature exceeds 90 degrees Celsius (194 degrees Fahrenheit). The internal equipment automatically shuts down the OC192 LR/STM64 LH 1550 laser when the card temperature rises to prevent the card from self-destructing.

**Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

### Procedure: Clear the AUTOLSROFF Alarm

**Step 1** If the temperature of the ONS 15454 SDH exceeds 90 degrees Celsius (194 degrees Fahrenheit), the alarm should clear if you solve the ONS 15454 SDH temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 1-60.

**Step 2** If the temperature of the ONS 15454 SDH is below 90 degrees Celsius (194 degrees Fahrenheit), the ONS 15454 SDH temperature is not the cause of the alarm, and you should replace the OC-192 card. Use the "Physically Replace a Card" procedure on page 1-110.

**Note**    When replacing a card with an identical type of card, no additional CTC provisioning is required.

**Step 3**  If card replacement does not clear the alarm, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.13 AUTORESET

- Minor (MN), Non-Service Affecting (NSA)

The Automatic System Reset alarm occurs when a card is performing an automatic warm reboot. An AUTORESET occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot.

⚠️

**Caution**  Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the AUTORESET Alarm

**Step 1**  Check for additional alarms that might have triggered an automatic reset.

**Step 2**  If the card automatically resets more than once a month with no apparent cause, replace it with a new card. Follow the "Physically Replace a Card" procedure on page 1-110.

✎

**Note**  When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 3**  If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.14 AUTOSW-AIS-SNCP

- Not Reported (NR) (Condition)

The Automatic SNCP Switch Caused by AIS condition indicates that automatic SNCP protection switching took place because of an AIS alarm. The SNCP is configured for revertive switching and will switch back to the working path after the fault clears.

The AIS condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but a node upstream on the circuit does not have its STM-N port in service.The upstream node often reports a loss of service, loss of frame, bit error signal degrade or failure, trace identifier mismatch, or an out-of-service port. The AUTOSW-AIS-SNCP clears when you clear the primary alarm on the upstream node.

To clear the condition, follow the procedure in the "MS-AIS" section on page 1-81. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.15  AUTOSW-LOP-SNCP

- Minor (MN), Service Affecting (SA)

An Automatic SNCP Switch Caused by LOP alarm indicates that automatic SNCP protection switching took place because of the LOP alarm. The SNCP is configured for revertive switching and will switch back to the working path after the fault clears.

## Procedure: Clear the AUTOSW-LOP-SNCP Alarm

**Step 1**  Verify the cabling and physical connections on the reporting card.

**Step 2**  If the alarm does not clear, perform a CTC reset on the reporting card. Follow the "Reset a Card in CTC" procedure on page 1-109.

**Step 3**  If the alarm does not clear, do a manual switch (side switch) to move traffic away from the card. Follow the "Side-Switch the Active and Standby Cross-Connect Card" procedure on page 1-108.

> **Note**  If you do not have a protect card for the reporting card, create a new circuit on the reporting card to achieve the same effect.

**Step 4**  Clear the manual switch. Follow the "Clear a Protection Group Switch Command" procedure on page 1-108.

**Step 5**  If the alarm persists, the problem is at the far-end node. Verify the stability of the cabling and physical connections that connect to the far-end card.

**Step 6**  If the alarm does not clear, do a CTC reset on the far-end card. Follow the "Reset a Card in CTC" procedure on page 1-109.

**Step 7**  If the alarm does not clear, do another CTC reset on the reporting card. Follow the "Reset a Card in CTC" procedure on page 1-109.

**Step 8**  If the alarm does not clear, switch from the far-end working card to the far-end protect card. Follow the "Lock Out an MS-SPRing Span" procedure on page 1-107.

**Step 9**  If the alarm persists, replace the far-end card. Use the "Physically Replace a Card" procedure on page 1-110.

> **Note**  When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 10**  If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.16  AUTOSW-SDBER-SNCP

- Not Alarmed (NA) (Condition)

The Automatic SNCP Switch Caused by Bit Error Rate Signal Degrade (SDBER) condition indicates that a signal degrade alarm caused automatic SNCP protection switching to occur. The SNCP is configured for revertive switching and will switch back to the working path after the signal degrade is resolved.

To clear the condition, follow the procedure in the "SDBER-EXCEED-HO" section on page 1-88. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.17  AUTOSW-SFBER-SNCP

- Not Alarmed (NA) (Condition)

The Automatic SNCP Switch Caused by Bit Error Rate Signal Failure (SFBER) condition indicates that a signal fail alarm caused automatic SNCP protection switching to occur. The SNCP is configured for revertive switching and will switch back to the working path after the signal fail is resolved.

To clear the condition, follow the procedure in the "SFBER-EXCEED-HO" section on page 1-90. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.18  AUTOSW-UNEQ-SNCP

- Minor (MN), Service Affecting (SA)

An Automatic SNCP Switch Caused by UNEQ alarm indicates that automatic SNCP protection switching took place because of an UNEQ alarm. The SNCP is configured for revertive switching and will switch back to the working path after the fault clears.

**Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

**Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the AUTOSW-UNEQ Alarm

**Step 1**    Display the CTC network view and right-click the span reporting AUTOSW-UNEQ. Select **Circuits** from the shortcut menu.

**Step 2**    If the specified circuit is a low-order path tunnel, check for low-order paths assigned to the tunnel.

**Step 3**    If the low-order path tunnel does not have assigned low-order paths, delete the low-order path tunnel from the list of circuits.

**Step 4**    If you have complete visibility to all nodes, check for incomplete circuits such as stranded bandwidth from circuits that were not deleted completely.

**Step 5**    If you find incomplete circuits, verify whether they are working circuits and if they are still passing traffic.

**Step 6**    If the incomplete circuits are not needed or are not passing traffic, delete them and log out of CTC. Log back in and check for incomplete circuits again. Recreate any needed circuits.

**Step 7**    If the alarm does not clear, verify that all circuits terminating in the reporting card are active.

    **a.**    In the node (default login) view, click the **Circuits** tab.

    **b.**    Verify that the State column lists the port as ACTIVE.

    **c.**    If the State column lists the port as INCOMPLETE, and the INCOMPLETE does not change after a full initialization, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

**Step 8**    After you determine that the port is active, verify the signal source received by the card reporting the alarm.

**Step 9**    If the alarm does not clear, check the far-end STM-N card that provides payload to the card.

**Step 10**    If the alarm does not clear, verify the far-end cross-connect between the STM-N card and the E-N card.

**Step 11**    If the alarm does not clear, clean the far-end optical fiber cable ends according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

⚠️

**Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

⚠️

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Step 12**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.19  BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)

The BKUPMEMP alarm refers to a problem with the Timing Communications and Control–International (TCC-I) card Flash memory. The alarm occurs when the TCC-I card is in use and has one of four problems: the Flash manager fails to format a Flash partition, the Flash manager fails to write a file to a

Flash partition, there is a problem at the driver level, or the code volume fails cyclic redundancy checking (CRC). CRC is a method to check for errors in data transmitted to the TCC-I. The BKUPMEMP alarm also raises the EQPT alarm. In this instance, use the following procedure to clear the BKUPMEMP and the EQPT alarm.

## Procedure: Clear the BKUPMEMP Alarm

**Step 1**   Verify that both TCC-I cards are powered and enabled by confirming the lit ACT/STBY LEDs on the TCC-I cards.

**Step 2**   If both TCC-I cards are powered and enabled, reset the active TCC-I card to make the standby TCC-I card active. Use the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

> **Note**   If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

Wait ten minutes to verify that the standby TCC-I does not reset by itself due to a code volume failure or other external failure. If the reset is not complete and error-free or if the standby TCC-I reboots by itself, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

**Step 3**   If the alarm clears, follow the "Reset the TCC-I using a Card Pull" procedure on page 4-7 on the new standby TCC-I and allow it to boot up completely.

**Step 4**   If the alarm does not clear, perform a second CTC reset, this time on the newly active TCC-I card to make the recently reseated standby TCC-I card active. Use the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the standby TCC-I does not reset itself. If the TCC-I reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

**Step 5**   If the alarm reappears after you perform the switch, replace the TCC-I card. Use the "Physically Replace a Card" procedure on page 1-110.

> **Note**   When replacing a card with an identical type of card, no additional CTC provisioning is required.

**Step 6**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.20  CARLOSS (EQPT)

- Minor (MN), Non-Service Affecting (NSA)

This carrier loss alarm means the ONS 15454 SDH and the workstation hosting CTC do not have a TCP/IP connection. It is a problem involving the LAN or data circuit used by the RJ-45 connector on the TCC-I card or the LAN backplane pin connection on the back of the ONS 15454 SDH. It does not involve an Ethernet circuit connected to a port on an Ethernet card. The problem is in the connection (usually a LAN problem) and not the CTC or the ONS 15454 SDH.

## Procedure: Clear the CARLOSS Alarm (EQPT)

**Step 1**   Verify connectivity by pinging the ONS 15454 SDH that is reporting the alarm.

   **a.**  If you are using a Microsoft Windows operating system, choose
**Start > Programs > Command Prompt**.

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

   **c.**  For both the Sun and Microsoft operating systems, at the prompt type:

      **ping [ONS 15454 IP address]**

      For example, ping 192.1.0.2.

   If the workstation has connectivity to the ONS 15454 SDH, it displays a "reply from [IP Address]" after the ping. If the workstation does not have connectivity, a "Request timed out" message displays.

**Step 2**   If the ping is successful, an active TCP/IP connection exists. Restart CTC.

**Step 3**   If you are unable to establish connectivity, perform standard network/LAN diagnostics.

For example, trace the IP route, check cables, and check any routers between the node and CTC.

**Step 4**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.21  CARLOSS (E-Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN alarm is the data equivalent of an SDH LOS alarm. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of this alarm are a disconnected straight-through (Category 5) LAN cable or an improperly installed Ethernet card. Ethernet card ports must be enabled (put in service) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

This alarm also occurs after the restoration of a node database. In this instance, the alarm will clear in approximately 30 seconds after spanning-tree protection reestablishes. This applies to the E-series Ethernet cards, but not to the G1000-4 card. The G1000-4 card does not use Spanning Tree Protocol (STP) and is unaffected by STP reestablishment.

⚠
**Caution**   Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the CARLOSS Alarm (E Series)

**Step 1**    Verify that the straight-through (Category 5) LAN cable is properly connected and attached to the correct port.

**Step 2**    If the straight-through (Category 5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an STM-N card.

**Step 3**    If there is no misconnection to an STM-N card, check 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 straight-through (Category 5) LAN cable connecting the transmitting device to the Ethernet port.

**Step 6**    If a valid Ethernet signal is present, physically reseat the Ethernet card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 7**    If the alarm does not clear, replace the Ethernet card. Use the "Physically Replace a Card" procedure on page 1-110.

> **Note**    When replacing a card with an identical type of card, no additional CTC provisioning is required.

**Step 8**    If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your particular network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect. If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm might 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, these steps do not apply.

> **Note**    A Ethernet manual cross-connect is used when another vendors' equipment sits between ONS 15454 SDHs, and the Open System Interconnection/Target Identifier Address Resolution Protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based data communications channel (DCC). To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an synchronous transport signal (STS) channel riding through the non-Cisco optical system network.

   **a.**   Right-click anywhere on the row of the CARLOSS alarm.

   **b.**   Click the **Select Affected Circuits** dialog 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 particular network, determine the ONS 15454 SDH and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

   • Log into the ONS 15454 SDH at the other end of the Ethernet manual cross-connect.

   • Double-click the Ethernet card that is part of the Ethernet manual cross-connect.

   • Click the **Circuits** tab.

- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. This circuit will connect the Ethernet card to an STM-N card on 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.

        If one of the circuit sizes is incorrect, follow the "Delete a Circuit" procedure on page 1-108.

    **f.** Reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 9** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.22  CARLOSS (G1000-4)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN alarm is the data equivalent of an SDH LOS alarm. The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-4 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. A common cause is that a straight-through (Category 5) LAN cable is not connected properly to the reporting Ethernet port, an STM-N card is connected to the port instead of an Ethernet device, or there is a problem with the signal from the Ethernet device attached to the G1000-4 port.

- There is a problem in the end-to-end path (including possibly the remote end G1000-4 card) that is causing the reporting G1000-4 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 this clears the CARLOSS on the reporting card. In this case, the CARLOSS alarm is normally accompanied by another alarm or condition on the end-to-end path, such as a TPTFAIL or an STM-N alarm or condition.

Refer to the "G1000-4 Card" section on page 3-91 for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TPTFAIL" section on page 1-102 for more information on alarms that occur when a point-to-point circuit exists between two G1000-4 cards.

Ethernet card ports must be enabled (put in service) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure: Clear the CARLOSS Alarm

**Step 1**    Verify that the straight-through (Category 5) LAN cable is properly connected and attached to the correct port.

**Step 2**    If the straight-through (Category 5) LAN cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an STM-N card.

**Step 3**    If there is no misconnection to the STM-N card, check that the transmitting attached Ethernet device is operational. If not, troubleshoot the device.

**Step 4**    If the alarm does not clear, use an Ethernet test set to determine that 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 straight-through (Category 5) LAN cable connecting the transmitting device to the Ethernet port.

**Step 6**    If link auto-negotiation is enabled on the G1000-4 port, but the auto-negotiation process fails, the G1000-4 turns off its transmitter laser and reports a CARLOSS alarm. If link auto-negotiation has been enabled for the port, check for conditions that could cause auto-negotiation to fail.

    **a.**    Confirm that the attached Ethernet device has auto-negotiation enabled and is configured for compatibility with the asymmetric flow control on the G1000-4.

    **b.**    Confirm that the attached Ethernet device configuration allows reception of flow control frames.

**Step 7**    If all previous attempts fail, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (This restarts the auto-negotiation process.)

**Step 8**    If the TPTFAIL alarm is also reported, see the "TPTFAIL" section on page 1-102. If the TPTFAIL alarm is not reported, continue to the next step.

> **Note**    When both alarms are reported, the reason for the condition might be the G1000-4's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

**Step 9**    If the TPTFAIL alarm was not reported, check to see whether terminal loopback has been provisioned on this port by clicking the **Conditions** tab and the **Retrieve Conditions** button and seeing if LPBKTERMINAL is listed for the port.

**Step 10**    If a loopback was provisioned, clear the loopback by following the "Clear a Loopback" procedure on page 1-108.

On the G1000-4 card, provisioning a terminal loopback causes the transmit laser to turn off. If an attached Ethernet device detects this as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could cause the CARLOSS alarm detected by the G1000-4 port in loopback.

If the port is not set in LPBKTERMINAL, continue to Step 11.

**Step 11**    If a CARLOSS alarm repeatedly appears and clears, examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect. If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm might be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, these steps do not apply.

> **Note** A Ethernet manual cross-connect is used when another vendors' equipment sits between ONS 15454 SDHs, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

    **a.** Right-click anywhere on the row of the CARLOSS alarm.

    **b.** Click the **Select Affected Circuits** dialog.

    **c.** Record the information in the type and size columns of the highlighted circuit.

    **d.** From the examination of the layout of your particular network, determine the ONS 15454 SDH and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

       – Log into the ONS 15454 SDH at the other end of the Ethernet manual cross-connect.

       – Double-click the Ethernet card that is part of the Ethernet manual cross-connect.

       – Click the **Circuits** tab.

       – Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. This circuit will connect the Ethernet card to an STM-N card on 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.

    If one of the circuit sizes is incorrect, follow the "Delete a Circuit" procedure on page 1-108.

    **f.** Reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide* for detailed procedures on how to create circuits.

**Step 12** If a valid Ethernet signal is present, physically reseat the Ethernet card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 13** If the alarm does not clear, replace the Ethernet card. Use the "Physically Replace a Card" procedure on page 1-110.

> **Note** When replacing a card with an identical type of card, no additional CTC provisioning is required.

**Step 14** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.23  CLDRESTART

    • Not Alarmed (NA) (Condition)

A Cold Restart condition occurs when you physically remove and insert a card, power up an ONS 15454 SDH, or replace a card.

⚠

**Caution**     Always use the supplied electrostatic discharge wristband when working with a powered
ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of
the shelf assembly.

## Procedure: Clear the CLDRESTART Condition

**Step 1**     If the condition fails to clear after the card reboots, physically reseat the card. Use the "Physically Reseat
a Card" procedure on page 1-110.

**Step 2**     If the condition does not clear, replace the card. Use the "Physically Replace a Card" procedure on
page 1-110.

✎

**Note**     When you replace a card with an identical type of card, you do not need to make any changes to
the database.

**Step 3**     If the condition does not clear, log into http://www.cisco.com/tac for more information or log into
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC
toll-free numbers for your country.

## 1.6.24  COMIOXC

- Critical (CR), Service Affecting (SA)

The Input/Output (I/O) Slot to Cross-Connect (XCON) Communication Failure alarm is raised by the 10
Gigabit Cross Connect (XC10G) card. It occurs when there is a communication failure for a particular
I/O slot.

## Procedure: Clear the COMIOXC Condition

**Step 1**     Follow the "Reset a Card in CTC" procedure on page 1-109 on the reporting XC10G card.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 2**     Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED
  depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 3**     If the CTC reset does not clear the alarm, move traffic off the XC10G card. Use the "Side-Switch the
Active and Standby Cross-Connect Card" procedure on page 1-108.

**Step 4**     Physically reseat the reporting card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 5**     If the alarm does not clear, replace the XC10G card. Use the "Physically Replace a Card" procedure on
page 1-110.

> **Note**    When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 6**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.25  CONTBUS-A-18

- Major (MJ), Non-Service Affecting (NSA)

The Communication Failure from TCC-I slot to TCC-I slot alarm means the main processor on the TCC-I card in Slot 7 has lost communication with the coprocessor on the second TCC-I card in Slot 11. The problem is with the physical path of communication from the TCC-I card to the reporting card. The physical path of communication includes the two TCC-I cards and the backplane.

> ⚠
> **Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

### Procedure: Clear the CONTBUS-A-18 Alarm

**Step 1**    Position the cursor over the TCC-I card in Slot 7 and reset it by following the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109 to make the TCC-I in Slot 11 active.

> **Note**    If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

**Step 2**    Wait approximately 2 minutes for the TCC-I in Slot 7 to reset as the standby TCC-I. Verify that the Standby LED is on before proceeding to the next step.

**Step 3**    Position the cursor over the TCC-I card in Slot 11 and follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109 to make the standby TCC-I in Slot 7 active.

**Step 4**    If the alarm reappears when the TCC-I in Slot 7 reboots as the active TCC-I, the TCC-I card in Slot 7 is defective and must be replaced by following the "Physically Replace a Card" procedure on page 1-110.

> **Note**    When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 5**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.26 CONTBUS-B-18

- Major (MJ), Non-Service Affecting (NSA)

The Communication Failure from TCC-I slot to TCC-I slot alarm means the main processor on the TCC-I card in Slot 11 lost communication with the coprocessor on the TCC-I card in Slot 7. The problem is with the physical path of communication from the TCC-I card to the reporting TCC-I card. The physical path of communication includes the two TCC-I cards and the backplane.

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the CONTBUS-B-18 Alarm on the TCC-I Card

**Step 1**    Position the cursor over the TCC-I card in Slot 11 and reset it by following the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109 to make the TCC-I in Slot 7 active.

✎

**Note**    If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

**Step 2**    Wait approximately 2 minutes for the TCC-I in Slot 11 to reset as the standby TCC-I. Verify that the Standby LED is on before proceeding to the next step.

**Step 3**    Position the cursor over the TCC-I card in Slot 7 and follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109 to make the standby TCC-I in Slot 11 active.

✎

**Note**    If the alarm reappears when the TCC-I in Slot 7 reboots as the active TCC-I, the TCC-I card in Slot 7 is defective and must be replaced. Follow the "Physically Replace a Card" procedure on page 1-110. When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 4**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.27 CONTBUS-IO-A

- Major (MJ), Service Affecting (SA)

A TCC-I A to Shelf Slot Communication Failure alarm occurs when the active TCC-I card in Slot 7 (TCC-I 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 might appear briefly when the ONS 15454 SDH switches to the protect TCC-I card. In the case of a TCC-I protection switch, the alarm clears after the other cards establish communication with the new active TCC-I card. If the alarm persists, the problem is with the physical path of communication from the TCC-I card to the reporting card. The physical path of communication includes the TCC-I card, the other card, and the backplane.

> ⚠️
>
> **Caution**   Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: 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 to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, complete the "Clear the MEA Alarm" procedure on page 1-76 for the reporting card.

**Step 2**   If the alarm object is any single card slot other than the standby TCC-I in Slot 11, perform a CTC reset of the traffic card. Use the "Reset a Card in CTC" procedure on page 1-109. Verify that the following LED behavior takes place:

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 3**   If the alarm object is the standby TCC-I in Slot 11, perform a soft reset of this card:

   **a.**   Right-click the Slot 11 TCC-I card.

   **b.**   Choose **Reset Card** from the shortcut menu.

   **c.**   Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 4**   If CONTBUS-IO-A is raised on several cards at once, complete the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the card you reset completely reboots. Verify that the standby LED is illuminated before proceeding to the next step.

**Step 5**   If the CTC reset does not clear the alarm, complete the "Physically Reseat a Card" procedure on page 1-110.

**Step 6**   If the reseated card has not rebooted successfully, or the alarm has not cleared, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service-affecting problem.

> ✎
>
> **Note**   If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

# 1.6.28 CONTBUS-IO-B

- Major (MJ), Non-Service Affecting (NSA)

A TCC-I B to Shelf Slot Communication Failure alarm occurs when the active TCC-I card in Slot 11 (TCC-I B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm might appear briefly when the ONS 15454 SDH switches to the protect TCC-I card. In the case of a TCC-I protection switch, the alarm clears after the other cards establish communication with the new active TCC-I card. If the alarm persists, the problem is with the physical path of communication from the TCC-I card to the reporting card. The physical path of communication includes the TCC-I card, the other card, and the backplane.

⚠️

**Caution**  Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: 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 to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, complete the "Clear the MEA Alarm" procedure on page 1-76 for the reporting card.

**Step 2**  If the alarm object is any single card slot other than the standby TCC-I in Slot 7, perform a CTC reset of the traffic card. Use the "Reset a Card in CTC" procedure on page 1-109. Verify that the following LED behavior takes place:

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 3**  If the alarm object is the standby TCC-I in Slot 7, perform a soft reset of this card:

  **a.**  Right-click the Slot 7 TCC-I card.

  **b.**  Choose **Reset Card** from the shortcut menu.

  **c.**  Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 4**  If CONTBUS-IO-B is raised on several cards at once, complete the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the card you reset completely reboots. Verify that the standby LED is illuminated before proceeding to the next step.

**Step 5**  If the CTC reset does not clear the alarm, complete the "Physically Reseat a Card" procedure on page 1-110.

**Step 6**  If the reseated card has not rebooted successfully, or the alarm has not cleared, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service-affecting problem.

**Note**    If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

## 1.6.29  CTNEQPT-PBPROT

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect Payload Bus alarm indicates a failure of the main payload between the protect cross-connect XC10G card in Slot 10 and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in either the cross-connect card, the reporting traffic card, or the backplane.

**Note**    If all traffic cards show this alarm, physically reseat the standby TCC-I card. If this fails to clear the alarm, replace the standby TCC-I card. Do not physically reseat an active TCC-I card. This disrupts traffic.

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

### Procedure: Clear the CTNEQPT-PBPROT Alarm

**Step 1**    Perform a CTC reset on the standby cross-connect XC10G card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 2**    Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

If the cross-connect reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

**Step 3**    If the alarm does not clear, physically reseat the standby cross-connect card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 4**    If the alarm does not clear and the reporting traffic card is the active card in the protection group, follow the "Move Protection Group Traffic with a Switch Command" procedure on page 1-107.

**Step 5**    Perform a CTC reset on the reporting card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.

- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 6**  Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 7**  If the alarm does not clear, physically reseat the reporting card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 8**  Follow the "Clear a Protection Group Switch Command" procedure on page 1-108.

**Step 9**  If the reporting traffic card is protect, perform a CTC reset on the reporting card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.

- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 10**  Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 11**  If the alarm does not clear, physically reseat the reporting card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 12**  If the alarm does not clear, replace the standby cross-connect card. Use the "Physically Replace a Card" procedure on page 1-110.

**Note**  When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 13**  If the alarm does not clear, replace the reporting traffic card. Use the "Physically Replace a Card" procedure on page 1-110.

**Step 14**  If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.30 CTNEQPT-PBWORK

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect Payload Bus alarm affects the main payload bus between the active cross-connect XC10G card in Slot 8 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, the reporting traffic card, or the backplane.

**Note**    If all traffic cards show this alarm, do a forced side switch on the active TCC-I card, as shown in Step 1, and physically reseat this TCC-I card. If this fails to clear the alarm, replace the TCC-I card. Do not physically reseat an active TCC-I card because it disrupts traffic.

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the CTNEQPT-PBWORK Alarm

**Step 1**    Follow the "Side-Switch the Active and Standby Cross-Connect Card" procedure on page 1-108 to move traffic from the active card to the standby cross-connect card.

**Note**    After the active cross-connect goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

**Step 2**    Perform a CTC reset on the reporting card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 3**    Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 4**    If the alarm does not clear, physically reseat the standby cross-connect card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Note**    The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.

**Step 5**    If the alarm does not clear and the reporting traffic card is the active card in the protection group, follow the "Move Protection Group Traffic with a Switch Command" procedure on page 1-107.

**Step 6**    Perform a CTC reset on the reporting card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 7**    Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 8**    If the CTC reset does not clear the alarm, physically reseat the reporting card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 9**    Follow the "Clear a Protection Group Switch Command" procedure on page 1-108.

**Step 10**   If the alarm does not clear, replace the cross-connect card. Use the "Physically Replace a Card" procedure on page 1-110.

> **Note**    When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 11**   If the alarm does not clear, replace the reporting traffic card. Use the "Physically Replace a Card" procedure on page 1-110.

**Step 12**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.31  DATAFLT

- Minor (MN), Non-Service Affecting (NSA)

The Software Fault or Data Integrity Fault alarm means that the database has exceeded the capacity of the Flash memory on the TCC-I.

> **Caution**   When the system reboots, the last configuration entered is not saved.

Log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.32  E3-ISD

- Not Alarmed (Condition)

The E3 Idle condition indicates that the E3-12 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. This condition occurs when the transmitting card is OOS-MNT. It is resolved when the OOS condition ends.

> **Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.33  EHIBATVG-A

- Major (MJ), Service Affecting (SA)

The Extreme High Voltage on Battery A alarm occurs when the voltage level on battery lead A exceeds –56.7 VDC in –48 VDC systems or –72 VDC in –60 VDC systems. The alarm indicates that the voltage on the battery lead is extremely high and power redundancy is no longer guaranteed. The alarm remains until the voltage remains below the threshold for 120 seconds.

The problem is external to the ONS 15454 SDH. Troubleshoot the power source for battery lead A. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.34  EHIBATVG-B

- Major (MJ), Service Affecting (SA)

The Extreme High Voltage on Battery B alarm occurs when the voltage level on battery lead B exceeds –56.7 VDC in –48 V DC systems or –72 VDC in –60 VDC systems. The alarm indicates that the voltage on the battery lead is extremely high and power redundancy is no longer guaranteed. The alarm remains until the voltage remains below the threshold for 120 seconds.

The problem is external to the ONS 15454 SDH. Troubleshoot the power source for battery lead B. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.35  ELWBATVG-A

- Major (MJ), Service Affecting (SA)

The Extreme Low Voltage on Battery Feed A alarm indicates the voltage is extremely low or has been lost, and power redundancy is no longer guaranteed. The alarm occurs when the voltage on battery feed A drops below –40.5 VDC in –48 VDC systems or –50 VDC in –60 VDC systems. The alarm clears when voltage has remained above –40.5 VDC for 120 seconds.

The problem is external to the ONS 15454 SDH. Troubleshoot the power source for battery lead A. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.36  ELWBATVG-B

- Major (MJ), Service Affecting (SA)

The Extreme Low Voltage on Battery Feed B alarm indicates the voltage is extremely low or has been lost, and power redundancy is no longer guaranteed. The alarm occurs when the voltage on battery feed B drops below –40.5 V DC in –48 V DC systems or –50 V DC in –60 V DC systems. The alarm clears when voltage has remained above –40.5 Vdc for 120 seconds.

The problem is external to the ONS 15454 SDH. Troubleshoot the power source for battery lead B. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.37 EOC

- Major (MJ), Non-Service Affecting (NSA)

The Termination Failure DCC alarm means the ONS 15454 SDH has lost the DCC. The DCC is three bytes, D1 through D3, in the SDH overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15454 SDH uses the DCC to communicate network management information.

⚠ **Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

⚠ **Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

⚠ **Warning**    **Invisible laser radiation may be emitted from the end of 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

⚠ **Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the EOC Alarm

**Step 1**    If an LOF (DS3, E-N, STM-N) alarm is also reported, first resolve the LOS alarm by following the troubleshooting procedure given for that alarm.

**Step 2**    If the alarm does not clear, on the node reporting the alarm, check the physical connections from the cards to the fiber-optic cables that are configured to carry DCC traffic.

**Step 3**    If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service ports by checking that the ACT LED on each STM-N card is on.

**Step 4**    If the ACT LEDs on CN-N cards are on, follow the "Check or Create Node SDCC Terminations" procedure on page 1-106 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 STM-N port is active and in service.

    **a.**    Confirm that the STM-N card shows a green LED by viewing CTC or viewing the physical card.

        A green LED indicates an active card. A yellow LED indicates a standby card.

    **b.**    To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

    **c.**    Click the **Provisioning > Line** tabs.

**d.** Verify that the State column lists the port as IS.

**e.** If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 7** If the STM-N card is in service, use an optical test set to check for signal failures on fiber terminations.

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

⚠️

**Caution** Using an optical test set disrupts service on the STM-N card. It might be necessary to manually switch traffic carrying circuits over to a protection path.

**Step 8** If there are no signal failures on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. See the *Cisco ONS 15454 SDH Installation and Operations Guide* for levels.

**Step 9** If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide* for more information.

**Step 10** If fiber connectors are properly fastened and terminated, reset the active TCC-I by following the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the standby TCC-I does not reset itself. If the TCC-I reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

✎

**Note** If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

Resetting the active TCC-I switches the traffic to the standby TCC-I. If the alarm clears when the ONS 15454 SDH switches to the standby TCC-I, the user can assume that the original active TCC-I is the cause of the alarm.

**Step 11** If resetting the TCC-I does not clear the alarm, replace the original active TCC-I with a new TCC-I card. Use the "Physically Replace a Card" procedure on page 1-110.

⚠️

**Caution** Resetting the active TCC-I can result in loss of traffic.

**Step 12** If the TCC-I replacement does not clear the alarm, delete the problematic SDCC termination.

**a.** Click the **Provisioning > SDH DCC** tabs.

**b.** Highlight the problematic SDCC termination.

**c.** Click **Delete**.

**d.** Click **Yes** at confirmation dialog box.

**Step 13** Recreate the SDCC termination.

**Step 14** Verify that both ends of the SDCC have been recreated at the optical ports.

**Step 15** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.38  EQPT

- Critical (CR), Service Affecting (SA)

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm is raised with a BKUPMEMP alarm, complete the procedure in the "BKUPMEMP" section on page 1-25. This procedure clears both the EQPT alarm and the BKUPMEMP alarm.

⚠ **Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

### Procedure: Clear the EQPT Alarm

**Step 1**    Perform a CTC reset on the reporting card. Use the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 2**    Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 3**    If the CTC reset does not clear the alarm, physically reseat the card. Use the "Physically Reseat a Card" procedure on page 1-110.

**Step 4**    If the physical reseat of the card fails to clear the alarm, replace the card. Use the "Physically Replace a Card" procedure on page 1-110.

✎ **Note**    When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 5**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.39  EQPT-MISS

- Critical (CR), Service Affecting (SA)

The Replaceable Equipment Unit is Missing alarm is reported against the fan-tray assembly unit. It indicates that a replaceable fan-tray assembly unit is missing or not fully inserted.

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered
ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge
of the shelf assembly.

## Procedure: Clear the EQPT-MISS Alarm

**Step 1**    If the alarm is reported against the fan object, check that the fan-tray assembly is present.

**Step 2**    If the fan-tray assembly is present, follow the "Physically Reseat Fan-Tray" procedure on page 1-110.

**Step 3**    If no fan-tray assembly is present, obtain a fan-tray assembly and refer to "Replace the Fan-Tray
Assembly" procedure on page 4-4.

**Step 4**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC
toll-free numbers for your country in order to report a service affecting problem.

# 1.6.40  E-W-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Misconnect East/West Direction alarm occurs when nodes in a ring have an East
slot/port misconnected to another East slot/port or a West slot/port misconnected to another West
slot/port. In most cases, the user did not connect the fiber cables correctly, or the ring provisioning plan
was flawed. You can physically reconnect the fiber cable to the correct slot/ports 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. Although the CTC method clears the alarm, it might change the
traditional East-West node connection pattern of the ring.

✎

**Note**    The E-W-MISMATCH alarm also appears during the initial setup of a ring with its East-West slot/ports
configured correctly. In this instance, the alarm clears itself shortly after the ring setup is complete.

✎

**Note**    The lower numbered slot on a node is traditionally labeled as the West slot. The higher numbered slot is
traditionally labeled as the East slot. For example, Slot 6 is West and Slot 12 is East.

## Procedure: 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**    Display the CTC network view and label each of the nodes on the diagram with the same name that
appears on the network map.

**Step 3**    Double-click each span to reveal the node name and slot/port for each end of the span.

**Step 4**    Label the span ends on the diagram with the same information.

For example, with Node 1/Slot12/Port1 - Node2/Slot6/Port1, label the end of the span that connects Node 1 and Node 2 at the Node 1 end "Slot 12/Port 1." Label the Node 2 end of that same span "Slot 6/ Port 1."

**Step 5**    Repeat Steps 3 and 4 for each span on your diagram.

**Step 6**    Label the highest numbered slot at each node "East" and the lowest numbered slot at each node "West."

**Step 7**    Look at the diagram. You should see a clockwise pattern of West slots connecting to East slots for each span.

**Step 8**    If any span has an East-to-West or West-to-West connection, physically switch the fiber cable connectors from the card that does not fit the pattern to the card that will continue the pattern. This should clear the alarm.

> **Note**    The physical switch procedure is the recommend method of clearing this alarm. This method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slot/ports as East and West. This is useful when the misconnected node is not geographically near the troubleshooter.

> **Warning**    **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

> **Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls and adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Step 9**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## Procedure: Clear the E-W-MISMATCH Alarm with CTC

**Step 1**    Log into the misconnected node. This is the node with both ring fibers misconnected; it is in the middle of the two nodes that have one of two ring fibers misconnected.

**Step 2**    Click the **Provisioning > MS-SPRing** tabs.

**Step 3**    From the row of information for the fiber span, use the "Identify a Ring ID or Node ID Number" procedure on page 1-105 to identify the node ID, ring ID, and the slot and port in the East Line list and West Line columns. Record this information before proceeding to Step 4.

**Step 4**    From the View menu, choose **Go to network view**.

**Step 5**    Delete and recreate the **MS-SPRing**.

    **a.**    Click the **Provisioning > MS-SPRing** tabs.

    **b.** Click the row from Step 3 to select it and click **Delete**.

    **c.** Click **Create**.

    **d.** Fill in the ring ID and node ID from the information collected in Step 3.

    **e.** Click **Finish** in the MS-SPRing Creation window.

**Step 6**    Display the CTC node (default login) view and click the **Maintenance > MS-SPRing** tabs.

**Step 7**    Change the West Line pull-down menu to the slot/port you recorded for the east line in Step 3.

**Step 8**    Change the East Line pull-down menu to the slot/port you recorded for the west line in Step 3.

**Step 9**    Click **OK**.

**Step 10**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.41  EXCCOL

- Minor (MN), Non-Service Affecting (NSA)

The Excessive Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 SDH unit and CTC might be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC-I card. This problem is external to the ONS 15454 SDH.

## Procedure: Clear the EXCCOL Alarm

Troubleshoot the network management LAN connected to the TCC-I card for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

**Step 1**    Verify that the network device port connected to the TCC-I card has a flow rate set to 10 Mb, half-duplex.

**Step 2**    If the alarm does not clear, troubleshoot the network device connected to the TCC-I card and the network management LAN.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.42  EXERCISE-RING-REQ

- Not Alarmed (NA) (Condition)

The Exercise Request on Ring condition is raised when optical cards in a two-fiber MS-SPRing are tested without switching traffic using the EXERCISE RING command. The condition clears on its own.

> **Note**    This is a condition and not an alarm. It does not require troubleshooting.

# 1.6.43  EXERCISE-SPAN-REQ

- Not Alarmed (NA) (Condition)

The Exercise Request on Span condition is raised when optical cards in a four-fiber MS-SPRing are tested without switching traffic using the EXERCISE SPAN command. The condition clears on its own.

> **Note**    This is a condition and not an alarm. It does not require troubleshooting.

# 1.6.44  EXT

- Minor (MN), Non-Service Affecting (NSA)

An External Facility alarm is detected externally from the node because an environmental alarm is present. For example, an open door or flooding can cause the alarm.

## Procedure: Clear the EXT Alarm

**Step 1**    Open the MIC-A/P card Maintenance tab to gather further information about this alarm.

**Step 2**    Perform your standard operating procedure for this environmental condition.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.45  EXTRA-TRAF-PREEMPT

- Major (MJ), Non-Service Affecting (NSA)

An Extra Traffic Preempted alarm is raised on STM-N cards because low-priority traffic directed to the protect system has been preempted. This is caused by a working system protection switch.

## Procedure: Clear the EXTRA-TRAF-PREEMPT Alarm

**Step 1**    Verify that the protection switch has occurred by checking the ring map.

**Step 2**    If a ring switch has occurred, clear the alarm on the working system by following the appropriate alarm procedure.

**Step 3**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.46 FAILTOSW

- Not Alarmed (NA) (Condition)

The Failure to Switch to Protection condition is raised when a working electrical card cannot switch to the protect card in a 1:N protection group, because another working electrical card with a higher priority alarm, is switched over and monopolizing the lone protect card.

## Procedure: Clear the FAILTOSW Condition

**Step 1**   Look up and troubleshoot the higher priority alarm. Clearing this alarm frees up the 1:N card and clears the FAILTOSW condition.

> **Note**   A higher priority alarm is an alarm raised on the working electrical card using the 1:N card protection group. This working electrical card is reporting an alarm, but not reporting a FAILTOSW alarm.

**Step 2**   If the condition does not clear, replace the working electrical card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 1-110. This card is the working electrical card using the 1:N card protection and not reporting FAILTOSW.

Replacing the working electrical card that is reporting the higher priority alarm allows traffic to revert back to this slot. This frees up the 1:N card, which can then take over traffic from the card reporting the lower priority alarm and the FAILTOSW alarm.

> **Note**   When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 3**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.47 FAILTOSW-HO

- Not Alarmed (NA) (Condition)

The Failure to Switch to Protection–High Order Path condition is raised when a working (or protect) STM-N card carrying high-order (VC-4 or VC-3) traffic cannot switch to the protect (or working) card because another electrical card with a higher priority alarm is switched over and is monopolizing the card.

## Procedure: Clear the FAILTOSW-HO Condition

**Step 1**  Look up and clear the higher priority alarm. For information on viewing alarms, refer to the *Cisco ONS 15454 SDH Installation and Operations  Guide*. Clearing this alarm frees the protection card and clears the FAILTOSW-HO condition.

> **Note**  A higher priority alarm is an alarm raised on the working STM-N card using the protection group. This working STM-N card is reporting an alarm, but not reporting a FAILTOSW-HO alarm.

**Step 2**  If the condition does not clear, replace the working STM-N card that is reporting the higher priority alarm. Follow the "Physically Replace a Card" procedure on page 1-110. Replacing the working (or protect) STM-N card that is reporting the higher priority alarm allows traffic to revert back to this slot. This frees up the protect (or working) card, which can then take over traffic from the card reporting the lower priority alarm and the FAILTOSW-HO alarm.

> **Note**  When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 3**  If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.48  FAILTOSW-LO

- Not Alarmed (NA) (Condition)

The Failure to Switch to Protection–Low-Order Path condition is raised when a working (or protect) STM-N card carrying low-order (VC-2 or VC-1) traffic cannot switch to the protect (or working) card because another working STM-N card with a higher priority alarm is switched over and is monopolizing the protect card.

## Procedure: Clear the FAILTOSW-LO Condition

**Step 1**  Look up and clear the higher priority alarm. For information on viewing alarms, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*. Clearing this alarm frees up the protect (or working) card and clears the FAILTOSW-LO condition.

> **Note**  A higher priority alarm is an alarm raised on the working STM-N card using the protection group. This working STM-N card is reporting an alarm, but not reporting a FAILTOSW-LO alarm.

**Step 2**   Replace the working STM-N card that is reporting the higher priority alarm. Follow the "Physically Replace a Card" procedure on page 1-110. Replacing the working (or protect) STM-N card that is reporting the higher priority alarm allows traffic to revert back to this slot. This frees up the protect (or working) card, which can then take over traffic from the card reporting the lower priority alarm and the FAILTOSW-LO alarm.

> ✎
>
> **Note**   When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 3**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.49  FAILTOSWR

- Not Alarmed (NA) (Condition)

The Ring Fail to Switch to Protection condition signals an APS ring switch failure. FAILTOSWR clears when one of the following actions occurs: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as a signal failure [SF] or signal degrade [SD] alarm) 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).**

> ⚠
>
> **Warning**   **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

### Procedure: Clear the FAILTOSWR Condition on a Four-Fiber MS-SPRing Configuration

**Step 1**   Check to see that every node expected to be part of the ring is listed in the ring map.

  **a.**   Click the **Provisioning > MS-SPRing** tabs.

  **b.**   Click the row of the affected ring under the West Switch column.

  **c.**   Select **Exercise Ring** in the drop-down list.

**Step 2**   If the condition does not clear, display the CTC network view.

**Step 3**   Look for alarms on STM-N cards that make up the ring or span and troubleshoot these alarms.

**Step 4**   Log into the near-end node and click the **Maintenance > MS-SPRing** tabs.

**Step 5**   Record the STM-N cards listed under West Line and East Line. Ensure these STM-N cards are active and in service.

    **a.**   Confirm that the STM-N card shows a green LED by viewing CTC or viewing the physical card.

       A green LED indicates an active card. A yellow LED indicates a standby card.

    **b.**   To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

    **c.**   Click the **Provisioning > Line** tabs.

    **d.**   Verify that the State column lists the port as IS.

    **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 6**   Verify fiber continuity to the ports on the recorded cards.

**Step 7**   Verify that the correct port is in service.

    **a.**   Confirm that the STM-N card shows a green LED by viewing CTC or viewing the physical card.

       A green LED indicates an active card. A yellow LED indicates a standby card.

    **b.**   To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

    **c.**   Click the **Provisioning > Line** tabs.

    **d.**   Verify that the State column lists the port as IS.

    **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

> ⚠️
> **Caution**   Using an optical test set disrupts service on the optical card. It might be necessary to manually switch traffic carrying circuits over to a protection path.

**Step 8**   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 9**   Clean the fiber according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 10**   Verify that the power level of the optical signal is within the STM-N card's receiver specifications. The *Cisco ONS 15454 SDH Installation and Operations Guide* lists these specifications.

**Step 11**   Repeat Steps 6 to 10 for any other ports on the card.

**Step 12**   Replace the protect standby STM-N card. Follow the "Physically Replace a Card" procedure on page 1-110.

**Step 13**   If the condition does not clear after you replace the MS-SPRing cards on this node one by one, follow Steps 4 to 12 for each of the nodes in the ring.

**Step 14**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.50  FAILTOSWS

- Not Alarmed (NA) (Condition)

The Span Failure to Switch to Protection condition signals an APS span switch failure. For four-fiber MS-SPRings, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS alarm does not appear. If the ring switch does not occur, the FAILTOSWS alarm appears. FAILTOSWS clears when one of the following actions occur: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as an SF or SD alarm) clears.

To clear the condition, follow the "Clear the FAILTOSWR Condition on a Four-Fiber MS-SPRing Configuration" procedure on page 1-51. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.51  FAN

- Critical (CR), Service Affecting (SA)

The Failure of the Cooling-Fan Tray alarm indicates a problem with the fan-tray assembly. When the fan is not fully functional, the temperature of the ONS 15454 SDH can rise above its normal operating range. The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the ONS 15454 SDH. However, even with five working fans, the fan tray can 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 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

### Procedure: Clear the FAN Alarm

**Step 1**    Check the condition of the air filter to see if it needs replacement. Refer to the "Air Filter Inspection" section on page 4-2.

**Step 2**    If the filter is clean, follow the "Physically Reseat Fan-Tray" procedure on page 1-110.

✏️

**Note**    The fan should run immediately when correctly inserted.

**Step 3**    If the fan does not run or the alarm persists, replace the fan tray. Follow the "Replace the Fan-Tray Assembly" procedure on page 4-4.

**Step 4**    If the replacement fan tray does not operate correctly, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.52 FE-EXERCISING-RING

- Not Alarmed (NA) (Condition)

The Far-End Exercising Ring condition is raised when far-end optical cards in a two-fiber MS-SPRing are being tested without switching traffic using the EXERCISE RING command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. The condition clears on its own.

**Note**    This is a condition and not an alarm. It does not require troubleshooting.

# 1.6.53 FE-EXERCISING-SPAN

- Not Alarmed (NA) (Condition)

The Far-End Exercising Span condition is raised when far-end optical cards in a four-fiber MS-SPRing are being tested without switching traffic using the EXERCISE SPAN command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. The condition clears on its own.

**Note**    This is a condition and not an alarm. It does not require troubleshooting.

# 1.6.54 FE-FRCDWKSWPR-RING

- Not Alarmed (NA) (Condition)

The Far-End Ring Working Facility Forced to Switch to Protection condition is raised from a far-end node when a ring is forced from the working system to the protect system using the FORCE RING command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both of the alarms or conditions clear when the main alarm clears.

## Procedure: 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 AIS alarm from the DS3i-N-12 card in Slot 16 of Node 1 might link to the main AIS alarm from an DS3i-N-12 card in Slot 16 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    View and clear the main alarm. Refer to the "Clear an MS-SPRing Span Command" procedure on page 1-107 for instructions.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.55 FE-FRCDWKSWPR-SPAN

- Not Alarmed (NA) (Condition)

The Far-End Working Facility Forced to Switch to Protection Span condition is raised from a far-end node when a span on a four-fiber MS-SPRing is forced from the working system to the protect system using the FORCE SPAN command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

## Procedure: 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 AIS alarm from the DS3i-N-12 card in Slot 16 of Node 1 might link to the main AIS alarm from an DS3i-N-12 card in Slot 16 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    View and clear the main alarm. Refer to the "Clear an MS-SPRing Span Command" procedure on page 1-107 for instructions.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.56 FE-LOCKOUTOFPR-SPAN

- Not Alarmed (NA) (Condition)

The Far-End Span Far End Lockout of Protection condition is raised when a bidirectional line switch ring (BSLR) span is locked out of the protection system from a far-end node using the LOCKOUT SPAN command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

## Procedure: 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 AIS alarm from the DS3i-N-12 card in Slot 16 of Node 1 might link to the main AIS alarm from an DS3i-N-12 card in Slot 16 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Click the **Maintenance > MS-SPRing** tabs.

**Step 4**    Click the MS-SPRing row in the West Switch column to reveal a pull-down menu and choose **CLEAR**.

**Step 5**   Click **Apply**. Click **Yes** on the confirmation dialog boxes. (Two confirmations are displayed.)

**Step 6**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.57  FE-MANWKSWPR-RING

- Not Alarmed (NA) (Condition)

The Far-End Ring Manual Switch of Working Facility to Protect condition is raised when an MS-SPRing working ring is switched from working to protect at a far-end node using the MANUAL RING command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

## Procedure: 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 AIS alarm from the DS3i-N-12 card in Slot 16 of Node 1 might link to the main AIS alarm from an DS3i-N-12 card in Slot 16 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**   View and clear the main alarm. Refer to the for instructions.

**Step 4**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.58  FE-MANWKSWPR-SPAN

- Not Alarmed (NA) (Condition)

The Far-End Span Manual Switch of Working Facility to Protect condition is raised when an MS-SPRing span is switched from working to protect at the far end using the MANUAL SPAN command. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting this AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

## Procedure: 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 AIS alarm from the DS3i-N-12 card in Slot 16 of Node 1 might link to the main AIS alarm from an DS3i-N-12 card in Slot 16 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    View and clear the main alarm. Refer to the "Clear an MS-SPRing Span Command" procedure on page 1-107 for instructions.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.59  FEPRLF

- Minor (MN), Non-Service Affecting (NSA)

The Far-End Protection Line Failure alarm means that there was an APS switching channel failure of signal on the protect card coming into the node.

**Note**    The FEPRLF alarm only is raised on the ONS 15454 SDH when 1+1 bidirectional protection is used on optical cards in a 1+1 configuration.

### Procedure: Clear the FEPRLF Alarm on an MS-SPRing

**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 alarm/condition on a card in Slot 16 of Node 1 might link to the main alarm from a card in Slot 16 in Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE alarm.

**Step 3**    View and clear the main alarm. Refer to the appropriate alarm section for instructions.

**Step 4**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.60  FORCED-REQ

- Not Alarmed (NA) (Condition)

The Force Switch Request on Facility or Equipment condition occurs when you enter the force command on a span or card to force traffic from a working card or working span to a protection card or protection span or vice versa. You do not need to clear this condition if you want the force switch to remain in place. To clear this condition, clear the force command.

## Procedure: Clear the FORCED-REQ Condition

**Step 1**  Click the **Maintenance** tab.

**Step 2**  Click the **Protection** tab for a card or span switch.

**Step 3**  At Operation, click the drop-down arrow.

**Step 4**  Choose **Clear** and click **Apply**.

**Step 5**  If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.61 FORCED-REQ-RING

- Not Alarmed (NA) (Condition)

The Force Switch Request on Ring condition applies to optical line cards when the FORCE RING command is applied to a two-fiber MS-SPRing to move traffic from the working system to the protect system, or vice versa.

To clear the condition, follow the "Clear the FORCED-REQ Condition" procedure on page 1-58. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.62 FORCED-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Force Switch Request on Span condition applies to optical line cards when the FORCE SPAN command is applied to an MS-SPRing to force traffic from working to protect or from protect to working.

To clear the condition, follow the "Clear the FORCED-REQ Condition" procedure on page 1-58. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.63 FRNGSYNC

- Major (MJ), Service Affecting (SA)

The Free-Running Synchronization Mode alarm means that the reporting ONS 15454 SDH is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the ONS 15454 SDH has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips might begin to occur on an ONS 15454 SDH that relies on an internal clock.

## Procedure: Clear the FRNGSYNC Alarm

**Step 1**    If the ONS 15454 SDH is configured to operate from its own internal clock, disregard this alarm.

**Step 2**    If the ONS 15454 SDH is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards.

**Step 3**    View and clear alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI and SYSBOOT.

**Step 4**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.64 FSTSYNC

- Minor (MN), Non-Service Affecting (NSA)

A Fast-Start Synchronization Mode alarm raises when the ONS 15454 SDH is choosing a new timing reference. The previous timing reference has failed. This alarm disappears after approximately 30 seconds.

**Note**    This is an informational alarm. No troubleshooting is required.

## 1.6.65 FULLPASSTHR-BI

- Not Alarmed (NA) (Condition)

The Bidirectional Full Pass-Through active condition is raised on a non-switching node for an MS-SPRing ring 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.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.66 HITEMP

- Critical (CR), Service Affecting (SA) (NE)
- Minor (MN), Non-Service Affecting (NSA) (EQPT)

The Equipment Failure from High Temperature alarm means the temperature of the ONS 15454 SDH is above 50 degrees Celsius (122 degrees Fahrenheit).

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the HITEMP Alarm

**Step 1**    View the temperature displayed on the ONS 15454 SDH LCD front panel on the upper-right corner. For an illustration of the LCD panel, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide.*

**Step 2**    Check that the temperature of the room is not abnormally high.

**Step 3**    Physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 SDH.

**Step 4**    Physically ensure that blank faceplates fill the ONS 15454 SDH empty slots. Blank faceplates help airflow.

**Step 5**    Check the condition of the air filter to see whether it needs replacement. Refer to the "Air Filter Inspection" section on page 4-2.

**Step 6**    If the filter is clean, follow the "Physically Reseat Fan-Tray" procedure on page 1-110.

✎

**Note**    The fan should run immediately when correctly inserted.

**Step 7**    If the fan does not run or the alarm persists, replace the fan tray. Follow the "Replace the Fan-Tray Assembly" procedure on page 4-4.

**Step 8**    If the replacement fan tray does not operate correctly, log into http://www.cisco.com/tac for more information. If the alarm does not clear, log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting condition.

# 1.6.67  HLDOVRSYNC

- Major (MJ), Service Affecting (SA)

Loss of the primary or secondary timing reference raises the Holdover Synchronization alarm. Timing reference loss occurs when line coding on the timing input is different from the configuration on the ONS 15454 SDH. It also usually occurs during the selection of a new node reference clock. The alarm indicates that the ONS 15454 SDH has gone into holdover and is using the ONS 15454 SDH internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

## Procedure: Clear the HLDOVRSYNC Alarm

**Step 1**    View and clear additional alarms that relate to timing, such as FRNGSYNC, FSTSYNC, HLDOVRSYNC, LOF (DS3, E-N, STM-N), LOS (DS-3, E-N, STM-N), MANSWTOINT, MANSWTOPRI, MANSWTOSEC, MANSWTOTHIRD, SYSBOOT, SWTOSEC, SWTOTHIRD, SYNC-FREQ (BITS, STM-N), SYNCPRI, SYSBOOT, and SYSBOOT.

**Step 2**     Reestablish a primary and secondary timing source according to local site practice.

**Step 3**     If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.68  HP-RFI

- Not Reported (NR) (Condition)

The High-Order Remote Failure Indication (RFI) condition indicates that there is a remote failure indication in the high-order (VC-4 or VC-3) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the RFI alarm in the reporting node.

## Procedure: Clear the HP-RFI Condition

**Step 1**     Log into the node at the far-end node of the reporting ONS 15454 SDH.

**Step 2**     Check for alarms, especially LOS.

**Step 3**     View and clear the main alarm. Refer to the appropriate alarm section for instructions.

**Step 4**     If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.69  HP-TIM

- Minor (MN), Service Affecting (SA)

The TIM High-Order Trace Identifier Mismatch Failure alarm indicates that the trace identifier J1 byte of the high-order (VC-4 or VC-3) overhead is faulty. This alarm is caused when there is a mismatch between the transmitted and received J1 identifier byte in the SDH path overhead. The error can originate in the transmit end or the receive end.

## Procedure: Clear the HP-TIM Alarm

**Step 1**     Use an optical test set capable of viewing SDH path overhead to determine the validity of the J1 byte.

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

**a.**     Examine the signal as near to the reporting card as possible.

**b.**     Examine the signal as close as possible to the output card.

**Step 2**     If the output card signal is valid, follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.70 HP-UNEQ

- Critical (CR), Service Affecting (SA)

The SLMF Unequipped High-Order Path unequipped alarm applies to the C2 path signal label byte in the high-order (VC-4 or VC-3) path overhead. This alarm is caused when no C2 byte is received in the SDH path overhead.

## Procedure: Clear the HP-UNEQ Alarm

**Step 1**    Use an optical test set capable of viewing SDH overhead to determine the validity of the C2 byte.

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

**a.** Examine signal as near the reporting card as possible.

**b.** Examine the signal as near the output card as possible.

**Step 2**    If the output card signal is valid, follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.71 IMPROPRMVL

- Critical (CR), Service Affecting (SA) (for active card)
- Minor (MN), Non-Service Affecting (NSA) (for standby card)

The procedural error improper removal alarm means a card was physically removed from its slot before the card was deleted in CTC. The card does not need to be in service to cause this alarm. It only needs to be recognized by CTC and the TCC-I card. This alarm does not appear if you delete the card from CTC before you physically remove the card from the node.

**Note**    CTC gives the user approximately 15 seconds to physically remove the card before CTC begins a card reboot.

**Caution**    Do not pull 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.

![Caution symbol] **Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the IMPROPRMVL Alarm

**Step 1**    In the CTC node view, right-click the card reporting the IMPROPRMVL.

**Step 2**    Choose **Delete** from the shortcut menu.

![Note symbol] **Note**    CTC does not allow you to delete this card if the card is in service, has a circuit mapped to it, is paired in a working/protection scheme, has DCC enabled, or is used as a timing reference.

**Step 3**    If the card is in service, take the facility out of service.

![Caution symbol] **Caution**    Before taking the facility out of service, ensure that no live traffic is present on the facility.

    **a.**    In the CTC node (default login) view, double-click the reporting card to display the card view.

    **b.**    Click the **Provisioning** tab.

    **c.**    Click the **State** column of any in-service ports.

    **d.**    Choose **OOS** to take the ports out of service.

**Step 4**    If a circuit has been mapped to the card, delete the circuit.

![Caution symbol] **Caution**    Before deleting the circuit, ensure that the circuit does not carry live traffic.

    **a.**    At the CTC node view, click the **Circuits** tab.

    **b.**    Click the applicable circuit, i.e., the circuit that connects to the reporting card.

    **c.**    Click **Delete**.

**Step 5**    If the card is paired in a protection scheme, delete the protection group.

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

    **b.**    Click the protection group of the reporting card.

    **c.**    Click **Delete**.

**Step 6**    If the card is provisioned for DCC, delete the DCC provisioning.

    **a.**    Click the **Provisioning > SDH DCC** tabs.

    **b.**    Click the slots and ports listed in DCC terminations.

    **c.**    Click **Delete** and click **Yes** in the confirmation box that appears.

**Step 7**    If the card is used as a timing reference, change the timing reference.

    **a.**    Click the **Provisioning > Timing** tabs.

    **b.**    Click the **Ref-1** menu.

    **c.**    Change Ref-1 from the listed STM-N card to **Internal Clock**.

    **d.**  Click **Apply**.

**Step 8**    Right-click the card reporting the IMPROPRMVL and choose **Delete**.

**Step 9**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.72  INHSWPR

- Not Alarmed (NA) (Condition)

The Inhibit Switch To Protect Request On Equipment condition is raised on line cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 protection scheme, traffic remains locked onto the working system. If the card is part of a1:N protection scheme, the traffic is not prevented from being switched to another card in the protection scheme unless each card was specifically locked on.

## Procedure: Clear the INHSWPR Condition

**Step 1**    In the CTC node (default login) view, click the **Maintenance > Protection** tabs.

**Step 2**    Under the Protection Groups column, click the group containing the card that is reporting the INHSWPR condition. The Selected Group column lists the status of all cards or ports in the group.

**Step 3**    Click the card or port that says LOCKED OUT.

**Step 4**    If the card or port is locked, click the **Unlock** button.

**Step 5**    If the card or port is switched, click the **Clear** button.

**Step 6**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.73  INHSWWKG

- Not Alarmed (NA) (Condition)

The Inhibit Switch To Working Request On Equipment condition is raised on line cards when the ability to switch to working has been disabled. If the card is part of a 1:1 protection scheme, traffic remains locked on to the protect system. If the card is part of a1:N protection scheme, the traffic is not prevented from being switched to another card in the protection scheme unless each card was specifically locked on.

## Procedure: Clear the INHSWWKG Condition

**Step 1**    In the CTC node (default login) view, click the **Maintenance > Protection** tabs.

**Step 2**    Under the Protection Groups column, click the group containing the card that is reporting the INHSWWKG condition. The Selected Group column lists the status of all cards or ports in the group.

**Step 3**    Click the card or port that says LOCKED OUT.

**Step 4**    If the card or port is locked, click the **Unlock** button.

**Step 5**    If the card or port is switched, click the **Clear** button.

**Step 6**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.74  INVMACADR

- Major (MJ), Non-Service Affecting (NSA)

The equipment failure Invalid MAC Layer Address alarm means the ONS 15454 SDH MAC address is invalid. The MAC address is permanently set into the ONS 15454 SDH chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADR.

## Procedure: Clear the INVMACADR Alarm

This is not a user-serviceable problem. Log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.75  KB-PASSTHR

- Not Alarmed (NA) (Condition)

The K Bytes Pass-Through Active condition is raised on a non-switching node for an MS-SPRing ring when the protect channels on the node are not active, and the node is in K Byte Pass-Through State due to a FORCE SPAN command.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.76  LKOUTPR-S

- Not Alarmed (NA) (Condition)

The Lockout of Protection condition is raised on a BSLR node when traffic is locked out of a working span using the LOCKOUT SPAN command.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.77 LKOUTWK-R

- Not Alarmed (NA) (Condition)

The Lockout of Working condition is raised on a BSLR node when traffic is locked on a working ring using the LOCKOUT-REQ-RING command.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.78 LKOUTWK-S

- Not Alarmed (NA) (Condition)

The Lockout of Working condition is raised on a BSLR node when traffic is locked on a working span using the LOCKOUT-REQ-SPAN command.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.79 LOCKOUT-REQ

- Not Alarmed (NA) (Condition)

The Lockout Switch Request on Facility/Equipment condition occurs when a user initiates a lockout switch request for an STM-N card or a lockout switch request on a SNCP at the path level. A lockout prevents protection switching from occurring. Clearing the lockout allows protection switching to take place again. Clearing the lockout switch request clears the LOCKOUT-REQ condition.

To clear the condition, follow the "Clear an SNCP Lockout" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.80 LOCKOUT-REQ-RING

- Not Alarmed (NA) (Condition)

The Lockout Switch Request On Ring condition is raised when a LOCKOUT RING command is applied to an MS-SPRing to keep traffic locked out of either working or protect systems.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.81 LOCKOUT-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Lockout Switch Request On Span condition is raised when a LOCKOUT SPAN command is applied to an MS-SPRing to lock traffic out of either a working or protect span.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.82 LOF (BITS)

- Major (MJ), Service Affecting (SA)

The Loss of Frame (LOF) alarm occurs when a port on the TCC-I BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 SDH has lost frame delineation in the incoming data.

**Note**     The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

**Caution**     Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

### Procedure: Clear the LOF Alarm

**Step 1**     Verify that the line framing and line coding match between the BITS input and the TCC-I.

    **a.** In CTC node (default login) view or card view, note the slot and port reporting the alarm.

    **b.** Find the coding and framing formats of the external BITS timing source. This should be in the user documentation for the external BITS timing source or on the timing source itself.

    **c.** Click the **Provisioning > Timing** tabs to display the General Timing window.

    **d.** Verify that the value listed in Coding matches the coding of the BITS timing source (either B8ZS or AMI).

    **e.** If the coding does not match, click **Coding** to reveal a menu. Choose the appropriate coding.

    **f.** Verify that the value listed in Framing matches the framing of the BITS timing source (either ESF or SF [D4]).

    **g.** If the framing does not match, click **Framing** to reveal the menu. Choose the appropriate framing.

**Note**     On the timing subtab, the binary 8-zero substitution (B8ZS) coding field is normally paired with Extended Superframe (ESF) in the Framing field, and the alternate mark inversion (AMI) coding field is normally paired with SF (D4) in the Framing field.

**Step 2**    If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC-I, replace the TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

> **Note**    When you replace a card with an identical type of card, you do not need to make any changes to the database.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.83  LOF (DS3, E-N, STM-N)

- Major (MJ), Service Affecting (SA)

An LOF alarm means the receiving ONS 15454 SDH has lost frame delineation in the incoming data. If, in this instance, the LOF appears on the E1-N-14 card or the E3-12 card, the framing of the transmitting equipment might be set to a format that differs from the receiving ONS 15454 SDH.

> **Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure:  Clear the LOF Alarm on DS3, E-N, or STM-N Card

**Step 1**    Verify that the line framing and line coding between the E1-N-14 port and the signal source match.

   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. Your network administrator has this information.

   c.  Display the card-level view of the reporting card.

   d.  Click the **Provisioning > Line** tabs.

   e.  Verify that the line type of the reporting port matches the line type of the signal source.

   f.  If the signal source line type does not match the reporting port, click **Type** and enter the correct type.

   g.  Click **Apply**.

**Step 2**    If the alarm does not clear when the coding and framing of the ONS 15454 SDH match the coding and framing of the signal source, replace the card.

> **Note**    When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.84 LOS (BITS)

- Major (MJ), Service Affecting (SA)

The TCC-I card has an LOS from the BITS timing source. An LOS occurs when an SDH receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

### Procedure: Clear the LOS Alarm

**Step 1**    Verify the wiring connection from the ONS 15454 SDH backplane BITS clock pin fields to the timing source.

**Step 2**    Check that the BITS clock is operating properly.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.85 LOS (DS-3, E-N, STM-N)

- Major (MJ), Service Affecting (SA)

An LOS for either a DS-3 port or a DS1-14 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

⚠

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

### Procedure: Clear the DS-3, E-N, or STM-N LOS Alarm

**Step 1**    Verify cabling continuity to the port.

**Step 2**    Verify that the correct port is in service.

    **a.**    Confirm that the STM-N card shows a green LED by viewing CTC or viewing the physical card.

A green LED indicates an active card. A yellow LED indicates a standby card.

b. To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the State column lists the port as IS.

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 3 Use an optical 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 4 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 5 If there is a valid signal, replace the DS-N connector on the ONS 15454 SDH.

Step 6 Repeat Steps 1 to 5 for any other port on the card that reports the LOS.

Step 7 Look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8 If there were no other alarms that might be the source of the LOS or if clearing such an alarm did not clear the LOS, replace the reporting card with the same type of card. Follow the "Physically Replace a Card" procedure on page 1-110.

Note When you replace a card with an identical type of card, you do not need change the CTC database.

Step 9 If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.86 LPBKFACILITY (DS-3, E-N, STM-N)

- Not Alarmed (NA) (Condition)

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information on loopbacks, see the "Network Troubleshooting Tests" section on page 2-1 or the "Identify Points of Failure on a Circuit Path" section on page 2-4.

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. You can provision loopbacks through CTC.

Caution The CTC permits loopbacks to be performed on an in-service circuit. This operation is service affecting.

## Procedure: Clear the LPBKFACILITY Condition

**Step 1**    From the CTC node (default login) view, double-click the reporting card to display the card view.

**Step 2**    Click the **Maintenance** tab.

**Step 3**    Follow the "Clear a Loopback" procedure on page 1-108.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.87  LPBKTERMINAL (DS-3, E-N, STM-N)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a suspect link or part of the network, and a signal comes back to the sending device. If the signal does not come back or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically isolate the source of the problem. For more information on loopbacks, see the "Network Troubleshooting Tests" section on page 2-1.

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far end equipment. You provision loopbacks using CTC.

## Procedure: Clear the LPBKTERMINAL Condition

**Step 1**    From the CTC node (default login) view, double-click the reporting card to display the card view.

**Step 2**    Click the **Maintenance** tab.

If the condition is reported against a DS3i-N-12 card, also click the **DS1** tab.

**Step 3**    Follow the "Clear a Loopback" procedure on page 1-108.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.88  LPBKTERMINAL(G1000-4)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software terminal loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter logically isolates the source of the problem. For more information on loopbacks, see the "Network Troubleshooting Tests" section on page 2-1.

G1000-4 cards only support Terminal loopbacks. When a port is set in terminal loopback, the outgoing signal being transmitted is fed back 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 fed back to the receive direction. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. Loopbacks are provisioned using CTC. CTC permits loopbacks on an in-service circuit. This operation is service affecting.

To clear the condition, follow the "Clear a Loopback" procedure on page 1-108. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.89  LP-PLM

- Minor (MN), Service Affecting (SA)

The SLMF-PLM Low-Order Path Label Mismatch alarm applies to the V5 byte in low-order (VC-2 or VC-1) path overhead. This alarm is caused when there is a mismatch between the transmitted and received V5 byte received in the SDH payload overhead.

## Procedure: Clear the LP-PLM Condition

**Step 1**    Use an optical test set capable of viewing SDH overhead to determine the validity of the V5 byte.

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

  **a.**  Examine signal as close to the reporting card as possible.

  **b.**  Examine the signal as close as possible to the card.

**Step 2**    If the output card signal is valid, follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.90  LP-RFI

- Not Reported (NR) (Condition)

The Low-Order RFI condition indicates that there is a remote failure indication in the low-order (VC-2 or VC-1) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the RFI alarm in the reporting node.

## Procedure: Clear the LP-RFI Condition

**Step 1**    Log into the far-end node of the reporting ONS 15454 SDH.

**Step 2**    Check for alarms, especially LOS.

**Step 3**    View and clear the alarms. Refer to the appropriate alarm section for the procedure.

**Step 4**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.91  LP-UNEQ

- Critical (CR), Service Affecting (SA)

The SLMF Unequipped Low-Order Path Unequipped alarm applies to the V5 byte in low-order (VC-2 or VC-1) path overhead. This alarm is caused when no V5 byte is received in the SDH payload overhead.

To clear the alarm, follow the "Clear the LP-PLM Condition" procedure on page 1-72. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.92  MAN-REQ

- Not Alarmed (NA) (Condition)

The Manual Switch Request on a Facility/Equipment condition occurs when a user initiates a manual switch request on an STM-N card or SNCP path. Clearing the manual switch clears the MAN-REQ alarm.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.93  MANRESET

- Not Alarmed (NA) (Condition)

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 alarm. This condition clears automatically, when the card finishes resetting.

**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.94 MANSWTOINT

- Not Alarmed (NA) (Condition)

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to the internal timing source.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.95 MANSWTOPRI

- Not Alarmed (NA) (Condition)

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary source.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.96 MANSWTOSEC

- Not Alarmed (NA) (Condition)

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to the secondary source.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.97 MANSWTOTHIRD

- Not Alarmed (NA) (Condition)

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the third source.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.98 MANUAL-REQ-RING

- Not Alarmed (NA) (Condition)

The Manual Switch Request On Ring condition occurs when a user initiates a MANUAL RING command on a two-fiber MS-SPRing ring to switch from working to protect or protect to working.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.99  MANUAL-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Manual Switch Request On Ring condition occurs when a user initiates a MANUAL SPAN command to move MS-SPRing traffic from a working span to a protect span, or vice versa.

To clear the condition, follow the "Clear an MS-SPRing Span Command" procedure on page 1-107. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.100  MEA (Bplane)

- Critical (CR), Service Affecting (SA)

The Mismatch of Equipment Attributes (MEA) alarm for the backplane means that the revision of the backplane is incompatible with XC10G equipment.

## Procedure: Clear the MEA Alarm

**Step 1**   If the MEA is also raised against other equipment, such as the AIP or a fan tray, troubleshoot these alarms first.

**Step 2**   If alarms are reported directly against the XC10G card, such as SWMTXMOD, troubleshoot these alarms next.

**Step 3**   Determine whether the ONS 15454 SDH shelf assembly is a newer European Telecommunications Standards Institute (ETSI) 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) or an earlier shelf assembly.

    **a.**   At the CTC node (default login) view, click the **Inventory** tab.

    **b.**   Under the Hardware Part # column, if the part number is 800-08708-XX, then you have a 10-Gbps-compatible shelf assembly (15454E-SA-ETSI).

    **c.**   Under the Hardware Part # column, if the number is not 800-08708-XX, then you are using an earlier shelf assembly.

**Step 4**   If the shelf assembly is not compatible with 10-Gbps equipment, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.101  MEA (EQPT)

- Critical (CR), Service Affecting (SA)

The Mismatch of Equipment Attributes alarm occurs when the physical card inserted in a slot does not match the card type that is provisioned for that slot in CTC. The alarm clears when the provisioned card type and the physical card type match.

## Procedure: Clear the MEA Alarm

**Step 1**  Determine whether the ONS 15454 SDH shelf assembly is a newer ETSI 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) or an earlier shelf assembly.

   **a.**  At the CTC node (default login) view, click the **Inventory** tab.

   **b.**  Under the Hardware Part # column, if the part number is 800-08708-XX, then you have a 10-Gbps-compatible shelf assembly (15454E-SA-ETSI).

   **c.**  Under the Hardware Part # column, if the number is not 800-08708-XX, then you are using an earlier shelf assembly.

**Step 2**  Read the name at the top of the card faceplate to physically verify that the type of card in the slot is the same type of card that is reported in the object column of the MEA row on the Alarms tab.

   **a.**  If you have a newer ETSI 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) and the card reporting the alarm is not an E1000-2-G or E100T-G, proceed to Step 3.

   **b.**  If you have a newer ETSI 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) and the card reporting the alarm is an E1000-2-G or E100T-12, then that version of the Ethernet card is incompatible and must be removed.

> ✎
>
> **Note**   The E1000-2-G and E100T-G cards are compatible with the newer ETSI 10-Gbps-compatible shelf assembly and are the functional equivalent of the older, non-compatible 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 ETSI 10-Gbps-compatible shelf assembly.

   **c.**  If you have an older, pre-ETSI shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later (which includes the XC10G, OC-192, E1000-2-G, E100T-G or OC-48 any slot [AS]), proceed to Step 3.

   **d.**  If you have an older, pre-ETSI shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later (which includes the XC10G, OC-192, E1000-2-G, E100T-G or OC-48 AS), the reporting card is incompatible with the shelf assembly and must be removed.

**Step 3**  On CTC, click the **Inventory** tab to reveal the provisioned card type.

**Step 4**  If you prefer the card type depicted by CTC, replace the physical card reporting the mismatch with the card type depicted by CTC (provisioned for that slot). Follow the "Physically Replace a Card" procedure on page 1-110.

**Step 5**  If you prefer the card that physically occupies the slot and the card is not in service, has no circuits mapped to it and is not part of a protection group, then put the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

**Note**  If the card is in service, has a circuit mapped to it, is paired in a working/protection scheme, has DCC communications enabled, or is used as a timing reference, then CTC does not allow you to delete the card.

**Step 6**  If the card is in service, take the facility out of service.

**Caution**  Before taking the facility out of service, ensure that no live traffic exists on the facility.

    **a.**  Double-click the reporting card to display the card view.

    **b.**  Click the **Provisioning** tab.

    **c.**  Click the State column of any in-service ports.

    **d.**  Choose **OOS** to take the ports out of service.

**Step 7**  If a circuit has been mapped to the card, follow the "Delete a Circuit" procedure on page 1-108.

**Caution**  Before deleting the circuit, ensure that no live traffic exists on the facility.

**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 http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.102  MEA (FAN)

- Critical (CR), Service Affecting (SA)

The Mismatch of Equipment Attributes alarm is reported against the fan tray when an older ONS 15454 SDH fan-tray assembly (FTA2) is used with certain cards that require the newer fan-tray assembly (15454E-FTA-48V). The 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) and fan-tray assembly (15454E-FTA-48V) are required with the ONS 15454 SDH OC192 LR/STM64 LH 1550, E1000-2-G, E100T-G, OC48 IR/STM16 SH AS 1310, or OC48 LR/STM16 AS 1550 cards.

## Procedure: Clear the MEA Alarm

**Step 1**   Determine whether the ONS 15454 SDH shelf assembly is a newer ETSI 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) or an earlier shelf assembly.

    **a.**   At the CTC node (default login) view, click the **Inventory** tab.

    **b.**   Under the Hardware Part # column, if the number is 800-08708-XX, then you have a 10-Gbps-compatible shelf assembly (15454-SA-10G).

    **c.**   Under the Hardware Part # column, if the number is not 800-08708-XX, then you are using an earlier shelf assembly.

**Step 2**   If you have a 10-Gbps-compatible shelf assembly (15454E-SA-ETSI), the alarm indicates that an older, incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5A fuse and follow the "Replace the Fan-Tray Assembly" procedure on page 4-4.

**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 follow the "Replace the Fan-Tray Assembly" section on page 4-4.

**Step 4**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.103 MEM-GONE

- Major (MJ), Non-Service Affecting (NSA)

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC-I card. CTC will not function properly until this alarm clears. The alarm clears when additional memory becomes available.

Log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.104 MEM-LOW

- Minor (MN), Non-Service Affecting (NSA)

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC-I card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC-I card is exceeded, CTC ceases to function.

Log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.105  MFGMEM

- Critical (CR), Service Affecting (SA)

The Manufacturing Data Memory Failure (MFGMEM) alarm raises if the ONS 15454 SDH cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC-I lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EEPROM on the AIP also stores the MAC address. Inability to read a valid MAC address disrupts IP connectivity and makes the ONS 15454 SDH icon on the CTC network view unavailable.

## Procedure: Clear the MFGMEM Alarm on the AIP

**Step 1**  Perform a CTC reset on the TCC-I card. Follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the standby TCC-I does not reset itself. If the TCC-I reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

> **Note**  If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

**Step 2**  If the alarm does not clear, perform a card pull reset on the TCC-I by referring to the "Reset the TCC-I using a Card Pull" procedure on page 4-7.

**Step 3**  If the alarm does not clear, physically replace the standby TCC-I card on the ONS 15454 SDH with a new TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

> **Note**  It takes up to 30 minutes for the active TCC-I to transfer the system software to the newly installed TCC-I. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the TCC-I LEDs flash to indicate failure and then the active/standby LED flashes. When the transfer completes, the TCC-I reboots and goes into standby mode after approximately three minutes.

**Step 4**  Reset the active TCC-I card. Follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the standby TCC-I does not reset itself. If the TCC-I reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

**Step 5**  Physically replace the remaining TCC-I card with the second TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

The ONS 15454 SDH boots up the second TCC-I card. The second TCC-I must also copy the system software, which can take up to twenty minutes.

**Step 6**  If the MFGMEM alarm continues to report after replacing the TCC-I cards, the problem lies in the EEPROM.

**Step 7** If the alarm persists, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.106 MFGMEM (Backplane or Fan)

- Critical (CR), Service Affecting (SA)

The Manufacturing Data Memory (EEPROM) failure alarm occurs if the ONS 15454 SDH cannot access the data in the EEPROM. This occurs when either the memory module on the component fails or the TCC-I loses the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. An inability to read a valid MAC address disrupts IP connectivity and makes the ONS 15454 SDH icon on the CTC network view unavailable.

## Procedure: Clear the MFGMEM Alarm on the Backplane or Fan Tray

**Step 1** Perform a CTC reset on the TCC-I card. Follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

✎ **Note** If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

**Step 2** If the alarm does not clear, perform a card pull reset on the TCC-I by referring to the "Reset the TCC-I using a Card Pull" section on page 4-7.

**Step 3** Physically replace the remaining TCC-I card with the second TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

✎ **Note** It takes up to 30 minutes for the active TCC-I to transfer the system software to the newly installed TCC-I. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the TCC-I LEDs flash to indicate failure and then the active/standby LED flashes. When the transfer completes, the TCC-I reboots and goes into standby mode after approximately three minutes.

**Step 4** Perform a CTC reset on the TCC-I card. Follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

**Step 5** Verify that the remaining TCC-I card is now in standby mode. (The ACT/STBY LED changes to amber.)

**Step 6** Physically replace the remaining TCC-I card with the second TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

**Step 7** If the MFGMEM alarm continues to report after replacing the TCC-I cards, the problem lies in the EEPROM.

**Step 8** If the MFGMEM is reported from the fan tray, replace the fan tray. Obtain a fan-tray assembly and follow the "Replace the Fan-Tray Assembly" procedure on page 4-4.

**Step 9**    If the MFGMEM is reported from backplane, or if the alarm persists after the fan tray is replaced, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service-affecting problem.

## 1.6.107  MS-AIS

- Not Reported (NR) (Condition)

The Multiplex Section AIS condition indicates that there is a defect at the line layer of the SDH overhead. The line layer refers to the segment between two SDH devices in the circuit and is also known as a maintenance span. The line layer deals with SDH payload transport, and its functions include multiplexing and synchronization.

This condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but the DS-3 or STM-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service, loss of frame, bit error signal degrade or failure, trace identifier mismatch, or an out-of-service port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

### Procedure: Clear the MS-AIS Condition

**Step 1**    View the main alarm.

**Step 2**    Clear the main alarm. Refer to the appropriate alarm section for instructions.

**Step 3**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.108  MS-RFI

- Not Reported (NR) (Condition)

The Multiplex Section (MS) Remote Fault Indication (RFI) condition indicates that the RFI condition is occurring at the line level. The line layer is the segment between two SDH devices in the circuit and is also known as a maintenance span. The line layer deals with SDH payload transport. The line layer functions include multiplexing and synchronization.

An RFI occurs when the ONS 15454 SDH detects an RFI in the SDH overhead because of a fault in another node. Resolving the fault in the adjoining node clears the MS-RFI condition in the reporting node.

### Procedure: Clear the MS-RFI Condition

**Step 1**    Log into the far-end node of the reporting ONS 15454 SDH.

**Step 2** Check for alarms, especially LOS.

**Step 3** View and clear the main alarm. Refer to the appropriate alarm section for the procedure.

**Step 4** If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.109  MSSP-OOSYNC

- Major (MJ), Service Affecting (SA)

The Procedural Error MS-SPRing Out of Synchronization alarm applies to the SDH NE ring. This alarm is caused when a node ring map is missing or changed.

**Warning** **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

**Warning** **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the MSSP-OOSYNC Alarm

**Step 1** Verify that each node has a unique node ID number by using the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 2** Repeat Step 1 for all nodes in the ring.

If two nodes have the same node ID number, use the "Change a Node ID Number" procedure on page 1-106 to change one node's ID number so that each node ID is unique.

**Step 3** If the ring map does not exist, click **Create**.

**Step 4** Create the ring. Choose two- or four-fiber, the node ID, and the East or West optical card as required.

**Step 5** Click **Yes** on the Create MSSPRing dialog box.

**Step 6** Check the fiber connections.

**Step 7** Clean the fiber according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 8** Follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 9** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.110 NOT-AUTHENTICATED

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

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred.

**Note** NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

# 1.6.111 PRC-DUPID

- Major (MJ), Non-Service Affecting (NSA)

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 SDH requires each node in the ring to have a unique node ID.

## Procedure: Clear the PRC-DUPID Alarm

**Step 1** Log into a node on the ring.

**Step 2** Find the node ID with the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 3** Repeat Step 2 for all the nodes on the ring.

**Step 4** If two nodes have an identical node ID number, use the "Change a Ring ID Number" procedure on page 1-105 o change one node ID number so that each node ID is unique.

**Step 5** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.112 PROTNA

- Minor (MN), Non-Service Affecting (NSA)

The Protection Unit Not Available alarm is raised by an out-of-service protection card when a TCC-I or XC10G card or port that is provisioned as part of a protection group is not available. This can occur when a card is reset, but clear as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

## Procedure: Clear the PROTNA Alarm

**Step 1** If the PROTNA alarm raises against a common control (TCC-I or XC10G) card and does not clear, ensure that a redundant control card is installed and provisioned in the chassis.

**Step 2** If the alarm is raised against a line card, check whether the facility has been taken out of service.

   **a.** In CTC, double-click the reporting card to display the card view (if the card is not an XC10G card).

   **b.** Click the **Provisioning** tab.

   **c.** Click the State column of any in-service ports.

   **d.** Choose **IS** to take the ports out of service.

**Step 3** Perform a CTC reset on the reporting card. Follow the "Reset a Card in CTC" procedure on page 1-109.

   • While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.

   • While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 4** Verify that the CTC reset is complete and error-free.

   • No new alarms appear in the Alarms tab on CTC.

   • If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.

   • If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 5** If the alarm persists, physically reseat the reporting card. Follow the "Physically Reseat a Card" procedure on page 1-110.

**Step 6** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.113  PWR-A

   • Major (MJ), Service Affecting (SA)

The NE Power Failure at Connector A alarm applies to the NE rack. This alarm is caused when no power is supplied to the main power connector. This alarm can be raised if power is connected to the backup power connector (connector B) but not to connector A, since power must be applied to both supplies.

**Warning** **Hazardous energy levels available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground/ metal objects will heat up and can cause serious burns or weld the metal objects to the terminals.**

## Procedure: Clear the PWR-A Alarm

**Step 1** Verify whether a power connection between the power source and power connector A is present.

**Step 2** Verify and reseat, if necessary, the connections between the power source and power connector A.

**Step 3** If the alarm cannot be cleared, verify the continuity of the power connection with a voltmeter using the procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 4** If the alarm cannot be cleared, verify the source power output with a voltmeter following the procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 5** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.114  PWR-B

- Major (MJ), Service Affecting (SA)

The NE Power Failure at Connector B alarm applies to the NE rack. This alarm is caused when no power is supplied to the backup power connector. This alarm can be raised if power is connected to the main power connector (connector A) but not to connector B, since power must be applied to both supplies.

**Warning**   **Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground. Metal objects will heat up and can cause serious burns or weld the metal object to the terminals.**

### Procedure: Clear the PWR-B Alarm

**Step 1**   Check whether a power connection is present between the power source and power connector B.

**Step 2**   Check and reseat, if necessary, the connections between the power source and power connector B.

**Step 3**   If the alarm cannot be cleared, verify the continuity of the power connection with a voltmeter using the procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 4**   If the alarm cannot be cleared, verify the source power output with a voltmeter following the procedures in the *Cisco ONS 15454 SDH Installation and Operations  Guide*.

**Step 5**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.115  RAI

- Not Alarmed (NA) (Condition)

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SDH path to the other. RAI on the DS3i-N-12 card indicates that far-end node is receiving a DS-3 or E-1AIS.

To clear the condition, follow the "AIS" procedure on page 1-14. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.116  RING-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Mismatched Ring alarm occurs when the ring ID of the ONS 15454 SDH that is reporting the alarm does not match the ring ID of another ONS node in the MS-SPRing. ONS nodes connected in an MS-SPRing must have identical ring IDs to function.

## Procedure: Clear the RING-MISMATCH Alarm

**Step 1** Log into the first node in the ring.

**Step 2** Check the ring ID. Follow the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 3** Note the number in the Ring ID field.

**Step 4** Log into the next ONS node in the MS-SPRing.

**Step 5** Check the ring ID. Follow the "Identify a Ring ID or Node ID Number" procedure on page 1-105.

**Step 6** If the ring ID matches the ring ID in the reporting ONS node, repeat Step 5 for the next ONS node in the MS-SPRing.

**Step 7** If the ring ID does not match the ring ID in the reporting ONS node, follow the "Change a Ring ID Number" procedure on page 1-105.

**Step 8** Verify that the ring map is correct.

**Step 9** Repeat Step 7 for all ONS nodes in the MS-SPRing.

**Step 10** If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.117 RING-SW-EAST

- Not Alarmed (NA) (Condition)

The Ring Switch is Active on the East Side condition occurs when a manual ring switch occurs at the east side of a two-fiber MS-SPRing. The condition clears when the switch is cleared.

**Note** This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.118 RING-SW-WEST

- Not Alarmed (NA) (Condition)

The Ring Switch is Active On the West Side condition occurs when a manual ring switch occurs at the west side of a two-fiber MS-SPRing. The condition clears when the switch is cleared.

**Note** This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.119 SD

- Not Alarmed (NA) (Condition)

A Signal Degrade (SD) condition occurs on optical STM-N lines and the low-order path termination when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the signal degrade threshold. Signal degrade is defined by Telcordia as a "soft failure" condition. SD and signal failure (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

A SD condition occurs for STM-N cards and the low-order path termination when the BER on the incoming optical line has passed the signal failure threshold in the range of $10^{-9}$ to $10^{-5}$. The condition travels on the B2 byte of the multiplexing section SDH overhead.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. 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.

**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).**

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

## Procedure: Clear the SD Condition

**Step 1**    Verify that the user-provisionable BER threshold is set at the expected level. Follow the "Verify BER Threshold Level" procedure on page 1-110.

**Step 2**    With an optical test set, measure the power level of the line to ensure it is within guidelines.

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

**Step 3**    Verify that optical receive levels are within the acceptable range.

**Step 4**    Clean the fiber according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 5**    Verify that single-mode fiber is used.

**Step 6**    Verify that a single-mode laser is used at the far end.

**Step 7**    If the problem persists, the transmitter at the other end of the optical line might be failing and require replacement.

**Step 8**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.120  SDBER-EXCEED-HO

- Not Alarmed, Service Affecting (SA)

The Signal Degrade Threshold Exceeded for High Order condition indicates that the signal degrade BER threshold has been exceeded for a high-order (VC-4 or VC-3) path on optical cards. This alarm is caused when the signal BER falls within the degrade threshold (typically 1E-7 dB) set on the node.

⚠ **Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

⚠ **Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the SDBER-EXCEED-HO Alarm

**Step 1**    Determine the BER threshold. Follow the "Verify BER Threshold Level" procedure on page 1-110.

**Step 2**    If it is acceptable in site practices, adjust the threshold.

Using an optical test set, measure the input power level of the line and ensure it is within the guidelines.

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

**Step 3**    Check input fiber cable connections to the reporting card.

**Step 4**    Clean the input fiber cable ends according to site practices.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.121  SF

- Not Alarmed (NA) (Condition)

A Signal Failure (SF) condition occurs on optical STM-N cards and the low-order path termination when the BER on the incoming optical line has passed the signal failure threshold in the range of $10^{-5}$ to $10^{-3}$. The alarm travels on the B2 byte of the multiplexing section SDH overhead; this alarm causes a protection switch at the line (facility) level.

The SF alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal failure is defined by Telcordia as a "hard failure" condition. SD and SF both monitor the incoming BER error rate and are similar alarms, but SF is triggered at a higher BER than SD.

**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).**

**Warning**    **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

## Procedure: Clear the SF Condition

**Step 1**    Verify that the user-provisionable BER threshold is set at the expected level. Follow the "Verify BER Threshold Level" procedure on page 1-110.

**Step 2**    Using an optical test set, measure the power level of the line and ensure it is within the guidelines.

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

**Step 3**    Verify that optical receive levels are within the acceptable range.

**Step 4**    Clean the fibers at both ends according to site practice for a line signal failure.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 5**    Verify that single-mode fiber is being used.

**Step 6**    Verify that a single-mode laser is being used at the far-end node.

**Step 7**    If the problem persists, the transmitter at the other end of the optical line might be failing and need replacement.

**Step 8**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.122 SFBER-EXCEED-HO

- Not Alarmed, Service Affecting (SA)

The Signal Failure Threshold Exceeded for High Order condition means that the signal fail BER threshold has been exceeded for a high-order (VC-4 or VC-3) path on optical cards. This alarm is caused when the signal BER falls past the fail threshold (typically 1E-4 dB) set on the node.

⚠ **Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

⚠ **Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures.**

## Procedure: Clear the SFBER-EXCEED-HO Condition

**Step 1**    Determine the BER threshold by clicking the card reporting the alarm, and clicking the **Provisioning** tab.

**Step 2**    If it is acceptable in site practices, adjust the threshold.

**Step 3**    Check the input power levels to the reporting card.

**Step 4**    Check input fiber cable connections to the reporting card.

**Step 5**    Clean the input fiber cable ends according to site practices.

If no practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.123 SFTWDOWN

- Minor (MN), Non-Service Affecting (NSA)

A Software Download in Progress alarm occurs when the TCC-I is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

⚠ **Caution**    It can take up to 30 minutes for software to be updated on a standby TCC-I card. Wait the full time period before removing the card. Premature removal can cause Flash corruption.

✎ **Note**    This is an informational alarm.

## 1.6.124 SNTP-HOST

- Minor (MN), Non-Service Affecting (NSA)

The Simple Network Time Protocol (SNTP) host failure alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. This failure can result from two causes: the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

### Procedure: 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.

**Step 2**   If the ping fails, contact the network administrator that manages the IP network supplying the SNTP information to the proxy and determine whether the network is experiencing problems which might affect the SNTP server/router connecting to the proxy ONS 15454 SDH.

**Step 3**   Ensure that the ONS 15454 SDH is provisioned correctly.

   **a.**   On the ONS node serving as the proxy, click the CTC **Provisioning > General** tabs.

   **b.**   Ensure the **Enable Proxy** check box is checked.

   **c.**   If the **Enable Proxy** check box is not checked, select this box to check it.

**Step 4**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.125 SPAN-SW-EAST

- Not Alarmed (NA) (Condition)

The Span Switch is Active on the East Side condition occurs when a force switch occurs at the east side of a four-fiber MS-SPRing span. The condition clears when the switch is cleared.

**Note**   This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.126 SPAN-SW-WEST

- Not Alarmed (NA) (Condition)

The Span Switch is Active on the West Side condition occurs when a force switch occurs at the west side of a four-fiber MS-SPRing span. The condition clears when the switch is cleared.

**Note**   This is a condition and not an alarm. It is for information only and does not require troubleshooting.

# 1.6.127 SQUELCH

- Not Alarmed (NA) (Condition)

The Ring Squelching Traffic condition occurs in an MS-SPRing 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 the circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The AU-AIS condition also appears on all nodes in the ring, except the isolated node.

⚠️ **Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

⚡ **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).**

⚡ **Warning** **Invisible laser radiation may 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 may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

## Procedure: Clear the SQUELCH Condition

**Step 1**  Determine the isolated node.

    **a.**  Display the CTC network view.

    **b.**  The dimmed node with red spans is the isolated node.

**Step 2**  Verify fiber continuity to the ports on the isolated node.

**Step 3**  Verify that the proper ports are in service.

    **a.**  Confirm that the STM-N card shows a green LED by viewing CTC or viewing the physical card.

        A green LED indicates an active card. A yellow LED indicates a standby card.

    **b.**  To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

    **c.**  Click the **Provisioning > Line** tabs.

    **d.**  Verify that the State column lists the port as IS.

    **e.**  If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 4**  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**   Verify that the power level of the optical signal is within the optical card's receiver specifications. Refer to the *Cisco ONS 15454 SDH Installation and Operations Manual* for card specifications.

**Step 6**   Ensure that the optical transmits and receives are connected properly.

**Step 7**   Replace the STM-N card. Follow the "Physically Replace a Card" procedure on page 1-110.

**Step 8**   If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.128  SSM-DUS

- Not Alarmed (NA) (Condition)

The Synchronization Status Message Quality level Changed to Do Not Use (DUS) occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. This type of signal can also be sent for line maintenance testing.

**Note**   This is a condition and not an alarm. It is for information only and does not require troubleshooting.

# 1.6.129  SSM-FAIL (BITS)

- Minor (MN), Non-Service Affecting (NSA)

The Failed to Receive Synchronization Status Message alarm means the synchronization status messaging (SSM) byte (S1 byte) of the SDH overhead multiplexing section received by the ONS 15454 SDH has failed. The problem is external to ONS 15454 SDH. The ONS 15454 SDH is set up to receive SSM, but the timing source is not delivering valid SSM messages.

## Procedure: Clear the SSM-FAIL Alarm

**Step 1**   Check that SSM is enabled on the external timing source.

**Step 2**   Use an optical test set to determine that the external timing source is delivering the SSM (S1) byte.

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

**Step 3**   If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.130  SSM-FAIL (STM-N)

- Minor (MN), Non-Service Affecting (NSA)

The Failed to Receive Synchronization Status Message alarm means the SSM byte (S1 byte) of the SDH overhead multiplexing section received by the ONS 15454 SDH has failed. The problem is external to ONS 15454 SDH. The ONS 15454 SDH is set up to receive SSM, but the timing source is not delivering valid SSM messages.

## Procedure: Clear the SSM-FAIL Alarm

**Step 1**    Check that SSM is enabled on the external timing source.

**Step 2**    Use an optical test set to determine that the external timing source is delivering the SSM (S1) byte.

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

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.131 SSM-LNC

- Not Alarmed (Condition)

The Local Node Clock (LNC) Traceable SSM condition means that the SSM (S1) byte of the SDH overhead multiplexing section has been changed to signify that the line or BITS timing source is LNC.

✎
**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.132 SSM-OFF (BITS)

- Not Alarmed (NA) (Condition)

The SSM Disabled on this Interface condition applies to references used for timing the node. It occurs when the SSM (S1) byte of the SDH overhead multiplexing section for this reference has been turned off. The ONS 15454 SDH is set up to receive SSM, but the timing source is not delivering SSM messages.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

To clear the condition, follow the "Clear the SSM-FAIL Alarm" procedure on page 1-93. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.133 SSM-OFF (STM-N)

- Not Alarmed (NA) (Condition)

The SSM Disabled on this Interface condition indicates that the SSM (S1) byte of the SDH multiplexing section overhead has been turned off. It applies to optical line cards. It occurs when SSM is off. The ONS 15454 SDH is set up to receive SSM, but the timing source is not delivering SSM messages.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

To clear the condition, follow the "Clear the SSM-FAIL Alarm" procedure on page 1-93. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.134  SSM-PRC

- Not Alarmed (Condition)

The Primary Reference Clock (PRC) Traceable SSM condition means that the SDH overhead multiplexing section S1 byte indicates the line or BITS timing source SSM has changed to PRC.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

# 1.6.135  SSM-SETS

- Not Alarmed (NA) (Condition)

The Synchronous Equipment Timing Source Traceable SSM condition means that the SSM (S1) byte indicates the line or BITS timing source has changed to SETS.

**Note**     This is a condition and not an alarm. It is for information only and does not require troubleshooting.

# 1.6.136  SSM-STU (BITS)

- Not Alarmed (NA) (Condition)

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not report the SSM S1 byte, but the ONS 15454 SDH has SSM support enabled. STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454 SDH.

SSM is a SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. SSM enables SDH devices to automatically choose the highest quality timing reference and to avoid timing loops.

## Procedure: Clear the STU Condition

**Step 1**    Click the **Provisioning > Timing** tabs.

**Step 2**    If the **Sync Messaging** check box is checked, uncheck it.

**Step 3**    If the **Sync Messaging** check box is unchecked, check it.

**Step 4**    Click **Apply**.

**Step 5**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.137  SSM-STU (STM-N)

- Not Alarmed (NA) (Condition)

The SSM Synchronization Traceability Unknown condition occurs when the reporting node is timed to a reference that does not report the SSM S1 byte, but the ONS 15454 SDH has SSM support enabled. STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454 SDH.

SSM is a SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. SSM enables SDH devices to automatically choose the highest quality timing reference and to avoid timing loops.

## Procedure: Clear the STU Condition

**Step 1**    Click the **Provisioning > Timing** tabs.

**Step 2**    If the **Sync Messaging** check box is checked, uncheck it.

**Step 3**    If the **Sync Messaging** check box is unchecked, check it.

**Step 4**    Click **Apply**.

**Step 5**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.138  SSM-TNC (BITS)

- Not Alarmed (NA) (Condition)

The SSM Transit Node Clock (TNC) Traceable condition occurs when the SSM quality level is changed to TNC.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.139 SSM-TNC (STM-N)

- Not Alarmed (NA) (Condition)

The SSM Transit Node Clock Traceable condition occurs when the SSM quality level is changed to TNC.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.140 SWMTXMOD

- Critical (CR), Service Affecting (SA)

The Switching Matrix Module Failure alarm occurs on the XC10G card or an I/O card. If the alarm reports against an I/O card, it means that the logic component on the cross-connect card is out of frame (OOF) with the logic component on the reporting I/O card. All traffic on the reporting I/O card is lost. If the alarm reports against an XC10G card, it means that a logic component internal to the reporting XC10G card is out of frame with a second logic component on the same XC10G card. One or more I/O cards might lose traffic as a result of this failure.

### Procedure: Clear the SWMTXMOD Alarm

**Step 1**    If the card reporting the alarm is the standby XC10G card, perform a CTC reset on the standby XC10G. Follow the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.
- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 2**    Verify that the CTC reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.
- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 3**    If the alarm persists, physically reseat the standby XC10G card. Follow the "Physically Reseat a Card" procedure on page 1-110.

**Step 4**    If the card reporting the alarm is the active XC10G card, follow the "Side-Switch the Active and Standby Cross-Connect Card" procedure on page 1-108 to move traffic from the active XC10G card to the standby XC10G card.

**Note**    After the active cross-connect goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

**Step 5**    If the card reporting the alarm is not the active XC10G card or if you completed the side switch in Step 4, perform a CTC reset on the reporting card. Follow the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.

- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 6**  Verify that the CTC reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 7**  If the alarm persists, physically reseat the standby XC10G card. Follow the "Physically Reseat a Card" procedure on page 1-110.

**Step 8**  If the card reporting the alarm is an I/O card, follow the "Side-Switch the Active and Standby Cross-Connect Card" procedure on page 1-108 to move traffic from the active cross-connect XC10G card to the standby cross-connect card.

**Step 9**  If the alarm does not clear after the cross-connect XC10G side switch, perform a CTC reset on the reporting card. Follow the "Reset a Card in CTC" procedure on page 1-109.

- While the card resets, the FAIL LED blinks on the physical card and then all LEDs turn off.

- While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 10**  Verify that the CTC reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is on.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Step 11**  If the alarm persists, physically reseat the reporting traffic/line card. Follow the "Physically Reseat a Card" procedure on page 1-110.

**Step 12**  If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

## 1.6.141  SWTOPRI

- Not Alarmed (NA) (Condition)

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 SDH switches to the primary timing source (reference 1). The ONS 15454 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 1.6.142  SWTOSEC

- Not Alarmed (NA) (Condition)

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 SDH has switched to the secondary timing source (reference 2). The ONS 15454 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

To clear the condition, view and clear alarms related to failures of the primary source, such as the SYNCPRI alarm. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.143 SWTOTHIRD

- Not Alarmed (NA) (Condition)

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 SDH has switched to the third timing source (reference 3). The ONS 15454 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

To clear the condition, view and clear alarms related to failures of the primary source, such as the SYNCPRI and SYSBOOT alarms. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.144 SYNC-FREQ (BITS, STM-N)

- Not Alarmed (NA) (Condition)

The Synchronization Reference Frequency Out Of Bounds condition is reported against any reference that is out of the bounds for valid references. The NE will fail this reference and choose another reference or internal to run on.

## Procedure: Clear the SYNC-FREQ Condition

**Step 1**    Use an optical test set to check 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 out of bounds, replace the TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

**Step 3**    If the SYNC-FREQ condition continues to report after replacing the TCC-I card, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.145  SYNCPRI

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 SDH loses the primary timing source (reference 1). The ONS 15454 SDH uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 SDH should switch to its secondary timing source (reference 2). This switch also triggers the SWTOSEC alarm.

## Procedure: Clear the SYNCPRI Condition

**Step 1**    From the CTC node (default login) view, click the **Provisioning > Timing** tabs.

**Step 2**    Check the current configuration for the REF-1 of the NE reference.

**Step 3**    If the primary reference is a BITS input, verify the wiring connection from the ONS 15454 SDH backplane BITS clock pin fields to the timing source.

**Step 4**    Check that the BITS clock is operating properly.

**Step 5**    If the primary reference clock is an incoming port on the ONS 15454 SDH, complete the procedure in the "LOF (DS3, E-N, STM-N)" section on page 1-68.

**Step 6**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.146  SYNCSEC

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 SDH loses the secondary timing source (reference 2). The ONS 15454 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 SDH should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454 SDH. This switch also triggers the SWTOTHIRD alarm.

## Procedure: Clear the SYNCSEC Alarm

**Step 1**    From the CTC node (default login) view, click the **Provisioning > Timing** tabs.

**Step 2**    Check the current configuration of the REF-2 for the NE Reference.

**Step 3**    If the secondary reference is a BITS input, verify the wiring connection from the ONS 15454 SDH backplane BITS clock pin fields to the timing source.

**Step 4**    Check that the BITS clock is operating properly.

**Step 5**    If the secondary timing source is an incoming port on the ONS 15454 SDH, complete the procedure in the "LOS (BITS)" section on page 1-69.

**Step 6**  If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.147  SYNCTHIRD

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 SDH loses the third timing source (reference 3). The ONS 15454 SDH uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15454 SDH uses an internal reference for source three, then the TCC-I card may have failed. The ONS 15454 SDH often reports either FRNGSYNC or HLDOVERSYNC alarms after a SYNCTHIRD alarm.

⚠️

**Caution**  Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the SYNCTHIRD Alarm

**Step 1**  From CTC node (default login) view, click the **Provisioning > Timing** tabs.

**Step 2**  Check the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 3**  If the third timing source is a BITS input, follow the procedure in the "LOS (BITS)" section on page 1-69.

**Step 4**  If the third timing source is an incoming port on the ONS 15454 SDH, follow the procedure in the "LOF (DS3, E-N, STM-N)" section on page 1-68.

**Step 5**  If the third timing source uses the internal ONS 15454 SDH timing, perform a CTC reset on the TCC-I card. Follow the "Reset Active TCC-I Card and Activate Standby Card" procedure on page 1-109.

Wait ten minutes to verify that the standby TCC-I does not reset itself. If the TCC-I reset is not complete and error-free or if the TCC-I reboots itself, log into http://www.cisco.com/tac for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

✎

**Note**  If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

**Step 6**  If this fails to clear the alarm, physically reseat the TCC-I card. See the "Reset the TCC-I using a Card Pull" section on page 4-7.

**Step 7**  If the CTC reset fails to clear the alarm, replace the TCC-I card. Follow the "Physically Replace a Card" procedure on page 1-110.

> ✎
>
> **Note**    When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 8**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

# 1.6.148 SYSBOOT

- Major (MJ), Service Affecting (SA)

The System Reboot alarm indicates that new software is booting on the TCC-I card. This is an informational alarm.

No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.149 TPTFAIL

- Major (MJ), Service Affecting (SA)

The Transport Layer Failure alarm indicates a break in the end-to-end Ethernet link integrity feature of the G1000-4 cards. This alarm indicates a far-end condition rather than a problem with the port reporting TPTFAIL.

This alarm indicates a problem, on either the SDH path or the remote Ethernet port, that prevents the complete end-to-end Ethernet path from working. If any SDH path alarm is on the SDH path used by the Ethernet port, the affected port raises a TPTFAIL alarm. If the far-end G1000-4 Ethernet port is administratively disabled or it is exhibiting a CARLOSS condition, it sets the C2 byte in the SDH path overhead to indicate a payload defect condition. This causes a TPTFAIL to be reported against this near-end port.

Another important point regarding a TPTFAIL condition is that the near-end port is automatically disabled (transmit laser turned off) when this condition occurs. This could cause the external Ethernet device attached at the near end to detect a downed link and turn off its transmitter. In turn, this would cause a CARLOSS condition on this port. In all cases the real problem is either in the SDH path being used by this G1000-4 port or in the far-end G1000-4 port to which it is mapped.

## Procedure: Clear the TPTFAIL Alarm

**Step 1**    An occurrence of TPTFAIL on a G1000-4 port indicates either a problem with the SDH path that this port is using or with the far end G1000-4 port that is mapped to this port. View and clear any alarms being reported by the STM-N card utilized by the Ethernet circuit of the G1000-4.

**Step 2**    If no alarms are reported by the STM-N card, the problem might be on the far-end G1000-4 port that the port reporting TPTFAIL is mapped to. Lookup and troubleshoot any alarms, such as CARLOSS, reported against the far-end port or card.

**Step 3**    If the alarm does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.150  TRMT

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Failure alarm occurs when there is a transmit failure on the E1-N-14 card because of an internal hardware failure. The card must be replaced.

⚠️

**Caution**    Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

## Procedure: Clear the TRMT Alarm on the E1-N-14 Card

**Step 1**    Replace the E1-N-14 card reporting the failure. Follow the "Physically Replace a Card" procedure on page 1-110.

✎

**Note**    When replacing a card with an identical type of card, you do not need to change the CTC database.

**Step 2**    If the alarm does not clear, log into http://www.cisco.com/tac to obtain information about handling the failed card or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country in order to report a service affecting problem.

# 1.6.151  TU-AIS

- Not Reported (NR) (Condition)

A Tributary Unit AIS means that there is an AIS, indicating a secondary condition, in the tributary overhead of the VC.

An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but the DS-3 or STM-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service, loss of frame, bit error signal degrade or failure, trace identifier mismatch, or an out-of-service port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

## Procedure: Clear the TU-AIS Condition

**Step 1**    Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports.

**Step 2**    View and clear the alarms. Refer to the appropriate alarm section for the procedure.

**Step 3**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.152  TU-LOP

- Not Reported (NR) (Condition)

A Tributary Unit LOP means that the first payload pointer in the SDH overhead is not synchronized according to the system clock.

⚠️ **Warning**    **The ONS 15454 SDH is a Class I (CDRH) and Class 1M (IEC) laser system.**

⚠️ **Warning**    **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.**

### Procedure: Clear the TU-LOP Alarm

**Step 1**    Check for LOS on the reporting card.

**Step 2**    On the card raising the alarm, check whether attenuation is present on the input fiber cable.

**Step 3**    Check the signal level on the input fiber with the attenuator (if present).

**Step 4**    If fiber signal level with the attenuator is below the correct threshold, remove the attenuator and check signal level again.

**Step 5**    If the signal level is still low, clean both ends of the fiber cable connection according to site practice.

If no site practice exists, follow the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" procedure on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" procedure on page 4-36, as appropriate.

**Step 6**    Clean the far-end optical fiber cable ends.

**Step 7**    If error remains, check for a timing alarm. Follow the procedure in the "SYNCPRI" section on page 1-100.

**Step 8**    If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.153  WKSWPR

- Not Alarmed (NA) (Condition)

The Working Switched To Protection condition is raised when a line experiences an LOS, signal fail, or signal degrade.

To clear the condition, follow the procedure in the "LOS (DS-3, E-N, STM-N)" section on page 1-69. If the condition does not clear, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

## 1.6.154  WTR

- Not Alarmed (NA) (Condition)

The Wait To Restore condition indicates that the following conditions exist: revertive switching is specified, a WKSWPR occurred, and although the working path is good again, the wait to restore the timer has not expired. The alarm clears when the timer expires and traffic is switched back to the working path.

**Note**    This is a condition and not an alarm. It is for information only and does not require troubleshooting.

# 1.7  Common Procedures in Alarm Troubleshooting

This section gives common procedures that are frequently used when troubleshooting alarms. For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

## Procedure: Identify a Ring ID or Node ID Number

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    From the View menu, choose **Go to network view**.

**Step 3**    Click the **Provisioning > MS-SPRing** tabs.

**Step 4**    From the Ring ID column, record the ring ID, or from the Nodes column, record the node IDs in the MS-SPRing. The node IDs are the numbers in parentheses next to the node name.

## Procedure: Change a Ring ID Number

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    From the View menu, choose **Go to network view**.

**Step 3**    Click the **Provisioning > MS-SPRing** tabs.

**Step 4**    Highlight the row of the ring and click **Edit**.

**Step 5**    In the MS-SPRing window, enter the new ID in the Ring ID field.

**Step 6**    Click **Apply**.

**Step 7**    Click **Yes** at the Changing Ring ID dialog box.

## Procedure: Change a Node ID Number

**Step 1** Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2** From the View menu, choose **Go to network view**.

**Step 3** Click the **Provisioning > MS-SPRing** tabs.

**Step 4** Highlight the ring and click **Edit**.

**Step 5** In the MS-SPRing window, right-click the node on the ring map.

**Step 6** Select **Set Node ID** from the shortcut menu.

**Step 7** Enter the new ID in the field.

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

## Procedure: Verify Node Visibility for Other Nodes

**Step 1** Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2** At the node (default) view, click the **Provisioning > MS-SPRing** tabs.

**Step 3** Highlight an MS-SPRing.

**Step 4** Click **Ring Map**.

**Step 5** Verify that each node in the ring appears on the ring map with a node ID and IP address.

**Step 6** Click **Close**.

## Procedure: Check or Create Node SDCC Terminations

**Step 1** Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2** At the node (default) view, click the **Provisioning > SDH DCC** tabs.

**Step 3** View the Port column entries to see where terminations are present for a node. If all terminations are not present, 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, if allowed** radio button.

   **d.** Verify that the **Disable OSPF on DCC Link** check box is unchecked.

   **e.** Click **OK**.

## Procedure: Lock Out an MS-SPRing Span

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    In the node (default CTC login view), click the **Maintenance > MS-SPRing** tabs.

**Step 3**    Click the MS-SPRing row table cell under the West Switch column to reveal the pull-down menu.

**Step 4**    Choose **LOCKOUT SPAN** and click **Apply**.

**Step 5**    Click **OK** on the MS-SPRing Operations dialog box.


## Procedure: Clear an MS-SPRing Span Command

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    In the node (default CTC login view), click the **Maintenance > MS-SPRing** tabs.

**Step 3**    Click the MS-SPRing row table cell under the West Switch column to reveal the pull-down menu.

**Step 4**    Choose **CLEAR** and click **Apply**.

**Step 5**    Click **OK** on the MS-SPRing Operations dialog box.


## Procedure: Clear an SNCP Lockout

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    From the View menu, choose **Go to network view**.

**Step 3**    Right-click the span where you want to clear the switch. Choose Circuits from the shortcut menu.

**Step 4**    On the Circuits on Span dialog box, choose CLEAR to remove a previously set switch command. Click **Apply**.

**Step 5**    In the Confirm SNCP Switch dialog box, click **Yes**.

**Step 6**    In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all SNCP circuits is CLEAR.


## Procedure: Move Protection Group Traffic with a Switch Command

**Step 1**    Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**    Display the CTC node (default login) view.

**Step 3**    At the CTC node (default login) view, click the **Maintenance > Protection** tabs.

**Step 4**    Double-click the protection group that contains the reporting card.

**Step 5**    Click the Working/Active card of the selected groups.

**Step 6**    Click **Switch**.

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

## Procedure: Side-Switch the Active and Standby Cross-Connect Card

**Step 1**    Log into a node on the network if you have not done so already.

**Step 2**    Display the CTC node (default login) view.

**Step 3**    Determine the active cross-connect card.

The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.

✎

**Note**    You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

**Step 4**    In the CTC node view, select the **Maintenance > XC Cards** tabs.

**Step 5**    Click **Switch**.

**Step 6**    Click **Yes** in the Confirm Switch dialog box.

## Procedure: Clear a Protection Group Switch Command

**Step 1**    Log into a node on the network if you have not done so already.

**Step 2**    Display the CTC node (default login) view.

**Step 3**    At the CTC node view, click the **Maintenance** > **Protection** tabs.

**Step 4**    Double-click the protection group that contains the reporting card.

**Step 5**    Highlight either selected group.

**Step 6**    Click **Clear** and click **Yes** at the confirmation dialog box.

## Procedure: Delete a Circuit

**Step 1**    Log into a node on the network if you have not done so already.

**Step 2**    Display the CTC node (default login) view.

**Step 3**    Click the circuit row to highlight it and click **Delete**.

**Step 4**    Click **Yes** at the Delete Circuits dialog box.

## Procedure: Clear a Loopback

**Step 1**    Log into a node on the network if you have not done so already.

**Step 2** Double-click the reporting card in CTC to display the card view.

**Step 3** Click the **Maintenance** tab.

**Step 4** In the Loopback Type column, look for any port row that displays a state other then None.

**Step 5** If a row contains a state other than None, click in the column cell to display the drop-down list and select **None**.

**Step 6** In the State column, look for any port row that displays a state other than INS.

**Step 7** If a row contains a state other than INS, click in the column cell to display the drop-down list and select **INS**.

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

## Procedure: Reset Active TCC-I Card and Activate Standby Card

**Step 1** Log into a node on the network if you have not done so already.

**Step 2** Identify the active TCC-I.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED of active TCC-I is green.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, the standby TCC-I has a green LED depiction with the letters "Act."

**Step 3** Right-click the active TCC-I.

**Step 4** Choose **Reset Card** from the shortcut menu.

**Step 5** Click **Yes** in the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and then all LEDs turn off.

While the card resets, a white LED with the letters "LDG" appears on the card in CTC.

**Step 6** Verify that the CTC reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is steadily lit amber.

- If you are looking at the CTC node (default login) view of the ONS 15454 SDH, a yellow LED depiction with the letters "Sby" has replaced the white "LDG" LED.

**Note** If CTC stops responding after performing a reset on the TCC-I, close the browser and start CTC again on the affected node.

## Procedure: Reset a Card in CTC

**Step 1** Log into a node on the network if you have not done so already.

**Step 2** Display the CTC node (default login) view.

**Step 3** Position the cursor over the slot reporting the alarm.

Step 4    Right-click and choose **RESET CARD** from the shortcut menu.

## Procedure: Verify BER Threshold Level

Step 1    Log into a node on the network if you have not done so already.

Step 2    Display the CTC node (default login) view.

Step 3    From the CTC node view, double-click the card reporting the alarm to display the card view.

Step 4    Click the **Provisioning > Line** tabs.

Step 5    Under the SD BER column on the **Provisioning** tab, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.

Step 6    If the entry is consistent with what the system was originally provisioned for, continue to Step 8.

Step 7    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 entry that is consistent with what the system was originally provisioned for.

Step 8    Click **Apply**.

## Procedure: Physically Replace a Card

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.

## Procedure: Physically Reseat a Card

Step 1    Open the card ejectors.

Step 2    Slide the card halfway out of the slot along the guide rails.

Step 3    Slide the card all the way back into the slot along the guide rails.

Step 4    Close the ejectors.

## Procedure: Physically Reseat Fan-Tray

Step 1    Use the retractable handles embedded in the front of the fan tray to pull the fan-tray assembly forward several inches.

**Step 2**    Push the fan-tray assembly firmly back into the ONS 15454 SDH.

**Step 3**    Close the retractable handles.

# General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454 SDH. To troubleshoot specific ONS 15454 SDH alarms, see Chapter 1, "Alarm Troubleshooting." If you cannot find what you are looking for in this chapter or Chapter 1, "Alarm Troubleshooting," contact the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

This chapter begins with the following sections on network problems:

- Network Troubleshooting Tests—Describes loopbacks and hairpin circuits, which you can use to test circuit paths through the network or logically isolate faults.

- Identify Points of Failure on a Circuit Path—Explains how to perform the tests described in the "Network Troubleshooting Tests" section.

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

- PC Connectivity Troubleshooting—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454 SDH

- CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC log-in or operation problems.

- CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC log-in or operation errors and PC and network connectivity.

- Circuits and Timing—Provides troubleshooting procedures for circuit creation, error reporting, and timing reference errors and alarms.

- Fiber and Cabling—Provides troubleshooting procedures for fiber and cabling connectivity errors.

## 2.1 Network Troubleshooting Tests

Use loopbacks and hairpins to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 SDH line (traffic) cards, except Ethernet cards, allow loopbacks and hairpins.

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

A facility loopback tests the line interface unit (LIU) of a card, the FMEC, and related cabling. After applying a facility loopback on a card, use a test set to run traffic over the loopback. A successful facility loopback eliminates the LIU, FMEC, or cabling as the potential cause of a network problem. Figure 2-1 shows a facility loopback on a E3-12 card.

*Figure 2-1    The facility loopback process on an E3-12 card*
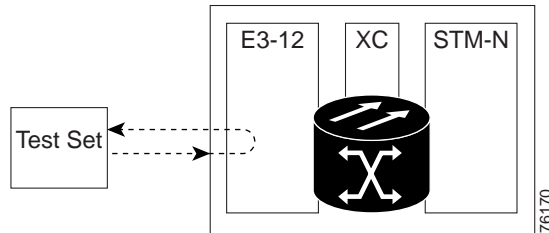


Figure 2-2 shows a facility loopback on a STM-N card.

⚠
**Caution**    Before performing a facility loopback on an STM-N card, make sure the card contains at least two SDCC paths to the node where the card is installed. A second SDCC path provides a non-looped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second SDCC is not necessary if you are directly connected to the ONS 15454 SDH containing the loopback OC-N.

*Figure 2-2    The facility loopback process on a STM-N card*
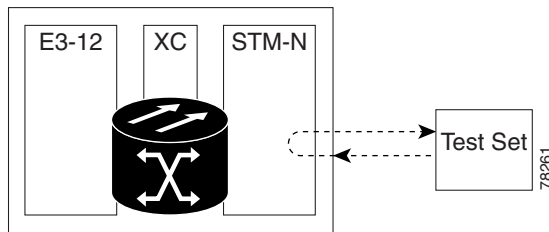


A terminal loopback tests a circuit path as it passes through the cross-connect card (XC10G) and as it loops back from the card being tested. Figure 2-3 shows a terminal loopback on an STM-N card. The test-set traffic comes in on the E3-12 card and goes through the cross-connect card to the STM-N card. The terminal loopback on the STM-N card turns the signal around before it reaches the LIU and sends it through the cross-connect card to the E3-12 card. This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the STM-N card.

*Figure 2-3    The terminal loopback process on an STM-N card*
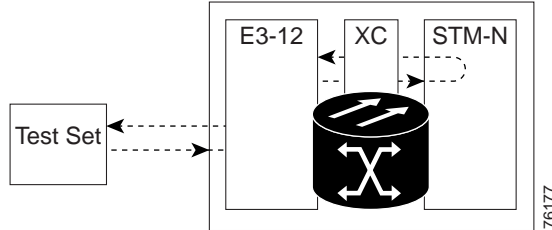


To test the LIU on an STM-N card, connect an optical test set to the STM-N card ports and perform a
facility loopback or use a loopback or hairpin on a card that is farther along the circuit path. Figure 2-4
shows a terminal loopback on an E3-12 card. The test-set traffic comes in on the STM-N card and goes
through the cross-connect card to the E3-12 card. The terminal loopback on the E3-12 card turns the
signal around before it reaches the LIU and sends it through the cross-connect card to the STM-N card.
This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the
E3-12 card.

*Figure 2-4    The terminal loopback process on an E3-12 card*
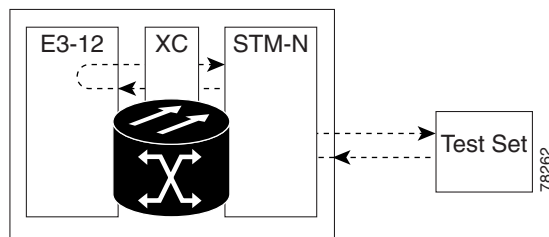


A hairpin circuit brings traffic in and out on an E3-12 port rather than sending the traffic onto the STM-N
card. A hairpin loops back only the specific E3 circuit and does not cause an entire STM-N port to loop
back, thus preventing a drop of all traffic on the STM-N port. The hairpin allows you to test a circuit on
nodes running live traffic. Figure 2-5 shows a hairpin circuit on an E3-12 card.

*Figure 2-5    The hairpin circuit process on an E3-12 card*
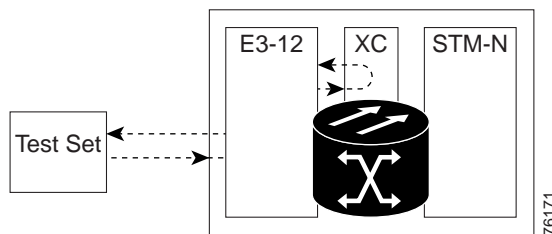
# 2.2  Identify Points of Failure on a Circuit Path

Facility loopbacks, terminal loopbacks, and hairpin circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a network test at each point along the circuit path systematically eliminates possible points of failure. The example in this section tests an E3-12 circuit on a two-node MS-SPRing. Using a series of facility loopbacks, terminal loopbacks, and hairpins, the path of the circuit is traced and the possible points of failure eliminated.

A logical progression of four network test procedures apply to this scenario:

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

1.  A facility loopback on the source-node E3-12 card

2.  A hairpin on the source-node E3-12 card

3.  A terminal loopback to the destination-node E3-12 card

4.  A facility loopback to the destination E3-12 card

✎    **Note**    All loopback tests require on-site personnel.

## 2.2.1  Perform a Facility Loopback on a Source E3-12 Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the E3-12 port in the source node. Completing a successful facility loopback on this port isolates the cabling, the E3-12 card, and the FMEC as possible failure points. Figure 2-6 shows an example of a facility loopback on a source E3-12 port.

The facility loopback test is performed on the source card in the network circuit, in this example, the source traffic card in the source node. Completing a successful facility loopback on this card eliminates the cabling, the E3-12 card, and the FMEC as possible failure points. shows an example of a facility loopback.

*Figure 2-6    A facility loopback on a circuit source E3-12 port*
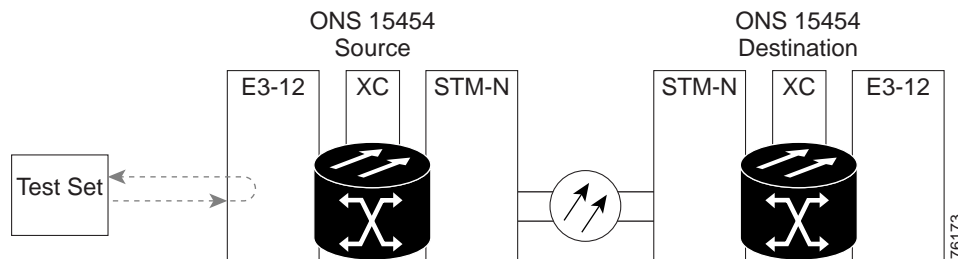


⚠    **Caution**    Performing a loopback on an in-service circuit is service-affecting.

## Procedure: Create the Facility Loopback on the Source E3-12 Port

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

    **a.** Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the FMEC connectors or DSx panel for the port you are testing. The transmit (Tx) and receive (Rx) terminals connect to the same port.

    **b.** Adjust the test set accordingly.

**Step 2** Use CTC to create the facility loopback circuit on the port being tested:

    **a.** In node view, double-click the card where you will perform the loopback.

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

    **c.** Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.

    **d.** 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.

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

    **f.** Click **Yes** in the Confirmation Dialog box.

> **Note** It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

**Step 3** Proceed to the "Test the Facility Loopback Circuit" section on page 2-5.

## Procedure: Test the Facility Loopback Circuit

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

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

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

Clear the loopback circuit before testing the next segment of the network circuit path.

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

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

    **c.** Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

    **d.** Click **Apply**.

    **e.** Click **Yes** in the Confirmation Dialog box.

Proceed to the "Perform a Hairpin on a Source Node Port" section on page 2-7.

**Step 4** If the test set indicates a faulty circuit, the problem may be a faulty E3-12 card, faulty cabling from the E3-12 card to the DSx panel or the FMEC, or a faulty FMEC.

Proceed to the "Test the E3-12 Cabling" section on page 2-6.

## Procedure: Test the E3-12 Cabling

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

- If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the DSx panel or the FMEC and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.

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

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

Replace the defective cable.

Clear the loopback circuit before testing the next segment of the network circuit path.

- **a.**  Click the **Maintenance > Loopback** tabs.
- **b.**  Choose **None** from the Loopback Type column for the port being tested.
- **c.**  Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
- **d.**  Click **Apply**.
- **e.**  Click **Yes** in the Confirmation Dialog box.

Proceed to the "Perform a Hairpin on a Source Node Port" section on page 2-7.

**Step 4**  If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty FMEC.

Proceed to the "Test the E3-12 Card" section on page 2-6.

## Procedure: Test the E3-12 Card

**Step 1**  Replace the suspect card with a known-good card. See "Card Replacement" section on page 4-17.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the faulty card. See "Card Replacement" section on page 4-17.

Clear the loopback circuit before testing the next segment of the network circuit path.

- **a.**  Click the **Maintenance > Loopback** tabs.
- **b.**  Choose **None** from the Loopback Type column for the port being tested.
- **c.**  Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
- **d.**  Click **Apply**.
- **e.**  Click **Yes** in the Confirmation Dialog box.

Proceed to the "Perform a Hairpin on a Source Node Port" section on page 2-7.

**Step 4**  If the test set indicates a faulty circuit, the problem may be a faulty FMEC.

Proceed to the "Test the FMEC Card" section on page 2-7.

## Procedure: Test the FMEC Card

**Step 1**    Replace the suspect card with a known-good card. See "Span Upgrade" section on page 4-24.

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

**Step 3**    If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

**Step 4**    If the test set indicates a good circuit, the problem is probably the defective FMEC card.

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the faulty card.

Clear the loopback circuit before testing the next segment of the circuit path.

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

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

**c.**    Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

**d.**    Click **Apply**.

**e.**    Click **Yes** in the Confirmation Dialog box.

Proceed to the "Perform a Hairpin on a Source Node Port" section on page 2-7.

## 2.2.2  Perform a Hairpin on a Source Node Port

The hairpin circuit test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 2-7 shows an example of a hairpin loopback on a source node port.

*Figure 2-7    Hairpin on a source node port*
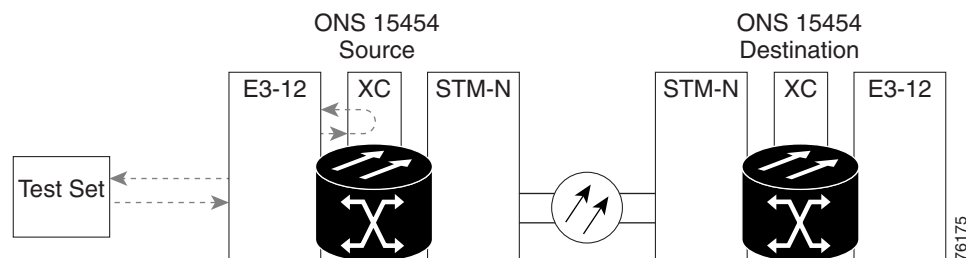
Note    The ONS 15454 SDH does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

## Procedure: Create the Hairpin on the Source Node

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

a.    If you just completed the "Perform a Facility Loopback on a Source E3-12 Port" section on page 2-4, leave the electrical test set hooked up to the E3-12 card.

b.    If you are starting the current procedure without the electrical test set hooked up to the E3-12 card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the FMEC card connectors for the port you are testing. The transmit (Tx) and receive (Rx) terminals connect to the same port.

c.    Adjust the test set accordingly.

Step 2    Use CTC to set up the hairpin on the port being tested:

a.    Click the **Circuits** tab and click the **Create** button.

b.    Give the circuit an easily identifiable name, such as hairpin1.

c.    Set the Circuit **Type** and **Size** to the normal preferences.

d.    Uncheck the **Bidirectional** checkbox and click **Next**.

e.    In the Circuit Source dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click **Next**.

f.    In the Circuit Destination dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click **Finish**.

Step 3    Confirm that the newly created circuit appears on the Circuits tab list as a 1-way circuit.

Step 4    Proceed to the "Test the Hairpin Circuit" section on page 2-8.

## Procedure: Test the 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 before testing the next segment of the network circuit path.

a.    Click the **Circuits** tab.

b.    Choose the hairpin circuit being tested.

c.    Click **Delete**.

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

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

Proceed to the "Perform a Terminal Loopback on a Destination E3-12 Port" section on page 2-10.

**Step 4**    If the test set indicates a faulty circuit, there may be a problem with the cross-connect card.

Proceed to the "Test the Alternate Cross-Connect Card" section on page 2-9.

## Procedure: Test the Alternate 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 screen, the ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

**Step 2**    Do a manual switch (side switch) of the cross-connect cards before retesting the loopback circuit:

⚠️

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

**a.** Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

✎

**Note**    After the active cross-connect goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

**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 loopback circuit before testing the next segment of the network circuit path.

**a.** Click the **Circuits** tab.

**b.** Choose the hairpin circuit being tested.

**c.** Click **Delete**.

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

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

Proceed to the "Perform a Terminal Loopback on a Destination E3-12 Port" section on page 2-10.

**Step 5**    If the test set indicates a good circuit, the problem may be a defective card.

To confirm a defective original cross-connect card, proceed to the "Retest the Original Cross-Connect Card" section on page 2-10.

## Procedure: Retest the Original Cross-Connect Card

**Step 1**   Do a manual switch (side switch) of the cross-connect cards to make the original cross-connect card the active card.

    **a.**  Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

**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 returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the defective cross-connect card. See "Card Replacement" section on page 4-17.

Clear the loopback circuit before testing the next segment of the network circuit path.

    **a.**  Click the **Circuits** tab.

    **b.**  Choose the hairpin circuit being tested.

    **c.**  Click **Delete**.

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

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

Proceed to the

**Step 4**   If the test set indicates a good circuit, the cross-connect card may have had a temporary problem that was cleared by the side switch.

Clear the loopback circuit before testing the next segment of the network circuit path.

    **a.**  Click the **Circuits** tab.

    **b.**  Choose the hairpin circuit being tested.

    **c.**  Click **Delete**.

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

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

Proceed to the

## 2.2.3  Perform a Terminal Loopback on a Destination E3-12 Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the E3-12 port in the destination node. First, create a bidirectional circuit that starts on the source node E3-12 port and loops back on the destination node E3-12 port. Then, proceed with the terminal loopback

test. Completing a successful terminal loopback to a destination node E3-12 port verifies that the circuit is good up to the destination E3-12. Figure 2-8 shows an example of a terminal loopback on a destination E3-12 port.

*Figure 2-8    Terminal loopback on a destination E3-12 port*
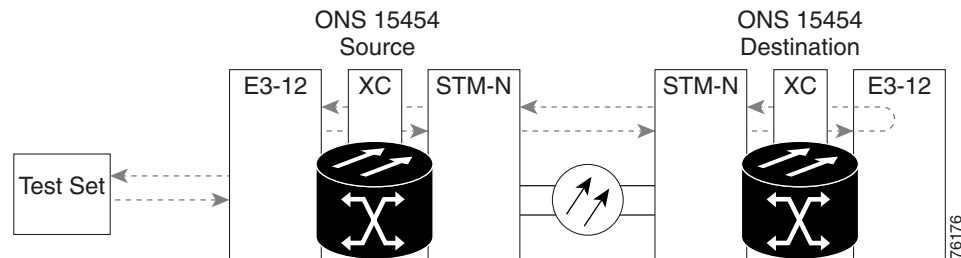


⚠

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

## Procedure: Create the Terminal Loopback on a Destination E3-12 Port

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

    **a.**    If you are starting the current procedure with the electrical test set hooked up to the E3-12 card in the source node, leave the test set hooked up.

    **b.**    If you are starting the current procedure without the electrical test set hooked up to the E3-12 card in the source node, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the FMEC card connectors for the port you are testing. Both transmit (Tx) and receive (Rx) cables connect to the same port.

    **c.**    Adjust the test set accordingly.

**Step 2**    Use CTC to set up the terminal loopback circuit on the port being tested.

    **a.**    Click the **Circuits** tab and click the **Create** button.

    **b.**    Give the circuit an easily identifiable name, such as E312toE312.

    **c.**    Set Circuit **Type** and **Size** to the normal preferences.

    **d.**    Leave the **Bidirectional** checkbox checked and click **Next**.

    **e.**    In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click **Next**.

    **f.**    In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the E3-12 port in the destination node) and click **Finish**.

**Step 3**    Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

✎

**Note**    It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

**Step 4**    Create the terminal loopback on the destination card and 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 pull-down list in the Select Node box and click **OK**.

**b.** In node view, double-click the card that requires the loopback, such as the E3-12 card in the destination node.

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

**d.** Select OOS_MT from the 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**   Proceed to the "Test the Terminal Loopback Circuit on the Destination E3-12 Card" section on page 2-12.

---

## Procedure: Test the Terminal Loopback Circuit on the Destination E3-12 Card

**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 before testing the next segment of the network circuit path.

**a.** Double-click the E3-12 card in the destination node with the terminal loopback.

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

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

**d.** Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

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

**f.** Click **Yes** in the Confirmation Dialog box.

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 box.

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

Proceed to the "Perform a Facility Loopback on a Destination E3-12 Port" section on page 2-13.

**Step 4**   If the test set indicates a faulty circuit, the problem may be a faulty card.

Proceed to the "Test the Destination E3-12 Card" section on page 2-13.

## Procedure: Test the Destination E3-12 Card

**Step 1**  Replace the suspect card with a known-good card. See the "Card Replacement" section on page 4-17.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the defective E3-12 card. See the "Card Replacement" section on page 4-17.

Clear the terminal loopback before testing the next segment of the network circuit path.

  **a.**  Double-click the E3-12 card in the destination node with the terminal loopback.

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

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

  **d.**  Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

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

  **f.**  Click **Yes** in the Confirmation Dialog box.

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 box.

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

Proceed to the "Perform a Facility Loopback on a Destination E3-12 Port" section on page 2-13.

## 2.2.4  Perform a Facility Loopback on a Destination E3-12 Port

The facility loopback test is performed on the node source port in the circuit, in this example, the destination E3-12 port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination node cabling, E3-12 card, LIU, or FMEC card is responsible for a faulty circuit. Figure 2-9 on page 2-14 shows an example of a facility loopback on a destination E3-12 port.

*Figure 2-9    Facility loopback on a destination E3-12 port*
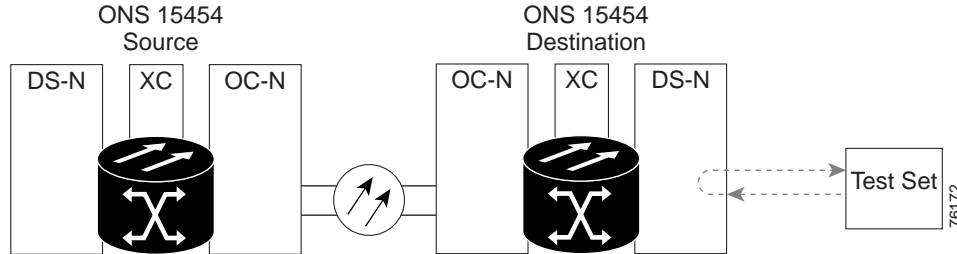


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

## Procedure: Create a Facility Loopback Circuit on a Destination E3-12 Port

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

   **a.**    Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the FMEC card connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.

   **b.**    Adjust the test set accordingly.

**Step 2**    Use CTC to create the facility loopback circuit on the port being tested:

   **a.**    In node view, double-click the card where the loopback will be performed.

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

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

   **d.**    Click **Apply**.

   **e.**    Click **Yes** in the Confirmation Dialog box.

✎
**Note**    It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

**Step 3**    Proceed to the "Test the Facility Loopback Circuit" section on page 2-14.

## Procedure: Test the Facility Loopback Circuit

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

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

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

   Clear the facility loopback.

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

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

    **c.** Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

    **d.** Click **Apply**.

    **e.** Click **Yes** in the Confirmation Dialog box.

The entire E3-12 circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

**Step 4** If the test set indicates a faulty circuit, the problem may be a faulty E3-12 card, faulty cabling from the E3-12 card to the DSx panel or the FMEC card, or a faulty FMEC card.

Proceed to the "Test the E3-12 Cabling" section on page 2-6.

## Procedure: Test the E3-12 Cabling

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

- If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the DSx panel or the FMEC card and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.

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

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

Replace the defective cable.

Clear the facility loopback.

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

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

    **c.** Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

    **d.** Click **Apply**.

    **e.** Click **Yes** in the Confirmation Dialog box.

The entire E3-12 circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

**Step 4** If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty FMEC card.

Proceed to the "Test the E3-12 Card" section on page 2-6.

## Procedure: Test the E3-12 Card

**Step 1** Replace the suspect card with a known-good card. See the "Card Replacement" section on page 4-17.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the faulty card. See the "Card Replacement" section on page 4-17.

Clear the facility loopback.

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

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

   **c.** Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

   **d.** Click **Apply**.

   **e.** Click **Yes** in the Confirmation Dialog box.

The entire E3-12 circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

**Step 4**   If the test set indicates a faulty circuit, the problem may be a faulty FMEC card.

Proceed to the "Test the FMEC Card" section on page 2-7.

## Procedure: Test the FMEC Card

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

   **a.** Remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 SDH, and pull it away from the shelf assembly.

   **b.** Loosen the nine perimeter screws that hold the backplane rear cover in place.

   **c.** Lift the FMEC card panel by the bottom to remove it from the shelf assembly.

   **d.** Follow the installation procedure for the appropriate FMEC card.

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

**Step 3**   If the test set indicates a good circuit, the problem is probably an improperly seated FMEC card.

Clear the facility loopback.

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

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

   **c.** Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

   **d.** Click **Apply**.

   **e.** Click **Yes** in the Confirmation Dialog box.

The entire E3-12 circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

**Step 4**   If the test set indicates a faulty circuit, the problem is probably the defective FMEC card.

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Replace the faulty FMEC card. See the "Card Replacement" section on page 4-17.

**Step 5**     Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement FMEC card.

**Step 6**     If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

If faulty circuit still persists, contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

**Step 7**     If the test set indicates a good circuit, the problem is probably the defective FMEC card.

Clear the facility loopback.

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

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

  **c.**   Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

  **d.**   Click **Apply**.

  **e.**   Click **Yes** in the Confirmation Dialog box.

The entire E3-12 circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

# 2.3  PC Connectivity Troubleshooting

This section contains troubleshooting procedures for PC and network connectivity to the ONS 15454 SDH.

## 2.3.1  Unable to Verify the IP Configuration of your PC

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

Table 2-1 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-1     Unable to Verify the IP Configuration of your PC*

| Possible Problem | Solution |
|---|---|
| The IP address was typed incorrectly. | Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. Refer to the "Verify the IP Configuration of your PC" section on page 2-18. |
| The IP configuration of your PC is not properly set. | To verify the IP configuration of your PC, refer to the "Verify the IP Configuration of your PC" section on page 2-18. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC. |

## Procedure: 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 Run window open field, type **command** and then click the **OK** button. The DOS command window will appear.

**Step 3**  At the prompt in the DOS window, type one of the following appropriate commands:

- For Windows 98, NT, and 2000, type **ipconfig** and press the **Enter** key.
- For Windows 95, type **winipcfg** and press the **Enter** key.

The Windows IP configuration information will be displayed, including the IP address, Subnet Mask, and the Default Gateway.

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

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

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

If you do not receive a reply, your IP configuration may not be properly set. Contact your Network Administrator for instructions to correct the IP configuration of your PC.

# 2.3.2  Browser Login Does Not Launch Java

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

Table 2-2 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-2    Browser Login Does Not Launch Java*

| Possible Problem | Solution |
|---|---|
| The PC operating system and browser are not properly configured. | Reconfigure the PC operating system java plug-in control panel and the browser settings. See the "Reconfigure the PC Operating System Java Plug-in Control Panel" section on page 2-18 and the "Reconfigure the Browser" section on page 2-19. |

## Procedure: 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 Control Panel** does not appear, the JRE may not be installed on your PC.

**a.**  Run the Cisco ONS 15454 SDH software CD.

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

**c.**  Double-click the j2re-1_3_1_02-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 1.3.1_02** icon.

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

**Step 6**    From the Java Run Time Environment menu, select
**JRE 1.3 in C:\ProgramFiles\JavaSoft\JRE\1.3.1_02**.

**Step 7**    Click the **Apply** button.

**Step 8**    Close the Java Plug-in Control Panel window.

## Procedure: 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** checkbox and click the **OK** button.

   **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:

   **g.**    For Windows 95/98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**

   **h.**    For Windows NT/2000, **C:\ProgramFiles\Netscape\<username>\Communicator\cache**.

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

   **j.**    Navigate to the file listed in f. and click the **OK** button.

   **k.**    Click the **OK** button 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 v1.3.1_02 for <applet> (requires restart)** checkbox.

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

**Step 4**    Temporarily disable any virus-scanning software on the computer. See the "Browser Stalls When Downloading CTC JAR Files From TCC-I" section on page 2-21.

**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 logon to the ONS 15454 SDH.

## 2.3.3  Unable to Verify the NIC Connection on your PC

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

Table 2-3 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-3     Unable to Verify the NIC Connection on your PC*

| Possible Problem | Solution |
|---|---|
| The Category 5 cable is not plugged in properly. | Confirm both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced. |
| The Category 5 cable is damaged. | Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending |
| Incorrect type of Category 5 cable is being used. | If connecting an ONS 15454 SDH directly to your laptop/PC or a router, use a straight-through Category 5 cable. When connecting the ONS 15454 SDH to a hub or a LAN switch, use a crossover Category 5 cable. |
| | For details on the types of Category 5 cables, see the "Crimp Replacement Category 5 Cables" section on page 2-44. |
| The NIC is improperly inserted or installed. | If you are using a PCMCIA based NIC, remove and re-insert the NIC to make sure the NIC is fully inserted. |
| | If the NIC is built into the laptop/PC, verify that the NIC is not faulty. |
| The NIC is faulty. | Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. |
| | If you have difficulty connecting to the network (or any other node), then the NIC may be faulty and needs to be replaced. |

## 2.3.4  Verify PC Connection to the ONS 15454 SDH (ping)

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

Table 2-4 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-4     Verify PC connection to ONS 15454 SDH (ping)*

| Possible Problem | Solution |
|---|---|
| A lost connection between the PC and the ONS 15454 SDH. | Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 SDH TCC-I card. A ping command will work if the PC connects directly to the TCC-I card or uses a LAN to access the TCC-I card. |
| | See the "Ping the ONS 15454 SDH" section on page 2-21. |

## Procedure: Ping the ONS 15454 SDH

**Step 1**    Display the command prompt:

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

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

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

```
ping [ONS 15454 SDH IP address]
For example, ping 192.1.0.2.
```

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

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

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

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

# 2.4  CTC Operation Troubleshooting

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

## 2.4.1  Browser Stalls When Downloading CTC JAR Files From TCC-I

**Symptom**   The browser stalls or hangs when downloading a CTC JAR file from the TCC-I card.

Table 2-5 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-5    Browser Stalls When Downloading jar File From TCC-I*

| Possible Problem | Solution |
| --- | --- |
| McAfee VirusScan software may be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later. | Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scan" section on page 2-22. |

## Procedure: 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 the **Configure** button 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** checkbox.

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

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

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

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

# 2.4.2  CTC Does Not Launch

**Symptom**  CTC does not launch, usually an error message appears before the login screen displays.

Table 2-6 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-6    CTC Does Not Launch*

| Possible Problem | Solution |
|---|---|
| The Netscape browser cache may point to an invalid directory. | Redirect the Netscape cache to a valid directory. See the "Redirect the Netscape Cache to a Valid Directory" section on page 2-22. |

## Procedure: Redirect the Netscape Cache to a Valid Directory

**Step 1** Launch Netscape.

**Step 2** Display the **Edit** menu.

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

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

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

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

## 2.4.3  Sluggish CTC Operation or Login Problems

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

Table 2-7 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-7    Sluggish CTC Operation or Login Problems*

| Possible Problem | Solution |
| --- | --- |
| The CTC cache file may be corrupted or may need to be replaced. | Delete the CTC cache file. This operation forces the ONS 15454 SDH to download a new set of jar files to your computer hard drive. See the "Delete the CTC Cache File Automatically" section on page 2-23 or the "Delete the CTC Cache File Manually" section on page 2-24. |

### Procedure: Delete the CTC Cache File Automatically

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

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

**Step 3**    Click the **Delete CTC Cache** button on the initial browser window to clear the CTC cache. Figure 2-10 shows the Delete CTC Cache screen.

**Note**    For CTC cache file manual deletion, see the "Delete the CTC Cache File Manually" section on page 2-24.

*Figure 2-10   Deleting the CTC cache*
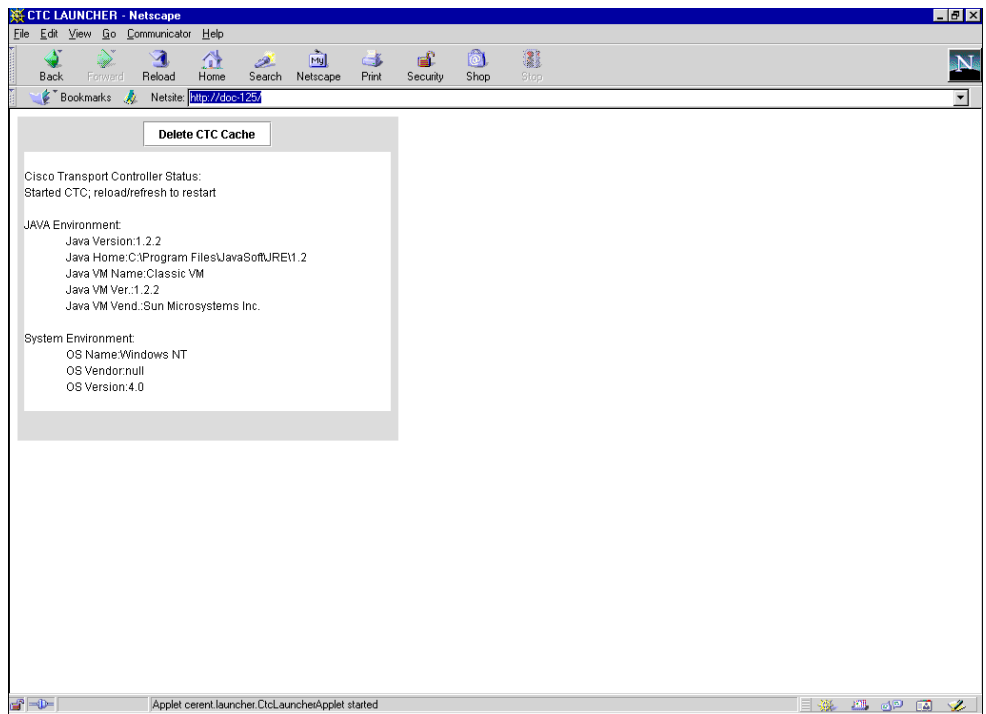


## Procedure: Delete the CTC Cache File Manually

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

**Step 2**  Enter *.jar in the Search for files or folders named field on the Search Results dialog box and click **Search Now**.

**Step 3**  Click the **Modified** column on the Search Results dialog box to find the jar files that match the date when you downloaded the files from the TCC-I. These files may include CTC*.jar, CMS*.jar, and jar_cache*.tmp.

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

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

# 2.4.4  Node Icon is Grey on CTC Network View

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

Table 2-8 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-8    Node Icon is Grey on CTC Network View*

| Possible Problem | Solution |
|---|---|
| Different CTC releases not recognizing each other. | Usually accompanied by an INCOMPATIBLE-SW alarm. Correct the core version build as described in the "Different CTC Releases Do Not Recognize Each Other" section on page 2-27. |
| A username/password mismatch. | Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the "Username or Password Does Not Match" section on page 2-28. |
| No IP connectivity between nodes. | Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "Ethernet Connections" section on page 2-30. |
| A lost DCC connection. | Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "Clear the EOC Alarm" procedure on page 1-42. |

## 2.4.5  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.

Table 2-9 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-9    CTC Cannot Launch Due to Applet Security Restrictions*

| Possible Problem | Solution |
|---|---|
| Did not execute the javapolicyinstall.bat file, or the java.policy file may be incomplete. | 1.  Verify that you have executed the javapolicyinstall.bat file on the ONS 15454 SDH software CD. This file is installed when you run the CTC Setup Wizard (refer to the CTC installation information in the *Cisco ONS 15454 SDH Installation and Operations Guide* for instructions). <br><br> 2.  If you ran the javapolicyinstall.bat file but still receive the error message, you must manually edit the java.policy file on your computer. See the "Manually Edit the java.policy File" section on page 2-25. |

## Procedure: Manually Edit the java.policy File

**Step 1**    Search your computer for this file and open it with a text editor (Notepad or Wordpad).

**Step 2**    Verify that the end of this file has the following lines:

```
    // Insert this into the system-wide or a per-user java.policy file.
  // DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!

  grant codeBase "http://*/fs/LAUNCHER.jar" {
permission java.security.AllPermission;
    };
```

**Step 3**    If these five lines are not in the file, enter them manually.

**Step 4**    Save the file and restart Netscape.

CTC should now start correctly.

**Step 5**    If the error message is still reported, save the java.policy file as (**.java.policy**). On Win95/98/2000 PCs, save the file to the C:\Windows folder. On WinNT4.0 PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

# 2.4.6  Java Runtime Environment Incompatible

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

Table 2-10 on page 2-26 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-10   Java Runtime Environment Incompatible*

| Possible Problem | Solution |
|---|---|
| Do not have the compatible Java 2 JRE installed. | The Java 2 Runtime Environment (JRE) contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. |
| | The ONS 15454 SDH CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 SDH software CD and on the Cisco ONS 15454 SDH documentation CD. See the "Launch CTC to Correct the Core Version Build" section on page 2-26. |
| | 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 2-11 shows JRE compatibility with ONS 15454 SDH software releases. |

*Table 2-11    JRE Compatibility*

| ONS Software Release | JRE 1.2.2 Compatible | JRE 1.3 Compatible |
|---|---|---|
| ONS 15454 SDH Release 3.3 | Yes | Yes |
| ONS 15454 SDH Release 3.4 | No | Yes |

## Procedure: Launch CTC to Correct the Core Version Build

**Step 1**    Exit the current CTC session.

**Step 2**    Click the **Delete CTC Cache** button in the browser window (Figure 2-10 on page 2-24).

**Step 3**    Completely close the browser.

**Step 4**    Start the browser.

**Step 5**    Type the ONS 15454 SDH IP address and click **Go**. This can be the original IP address you logged on with or an IP address other than the original.

**Step 6**    Log into CTC. The browser will download the jar file from CTC.

> **Note**    The .jar files consist of core and element files. Core files are common to the ONS 15454 SDH, ONS 15454 SONET, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15454 SDH Release 1.0 uses a 3.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

## 2.4.7  Different CTC Releases Do Not Recognize Each Other

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

Table 2-12 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-12    Different CTC Releases Do Not Recognize Each Other*

| Possible Problem | Solution |
|---|---|
| The software loaded on the connecting workstation and the software on the TCC-I card are incompatible. | This occurs when the TCC-I 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.<br><br>**Note**    Remember to always logon to the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 3.3 and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node will not recognize the new node.<br><br>See the "Launch CTC to Correct the Core Version Build" section on page 2-27. |

### Procedure: Launch CTC to Correct the Core Version Build

**Step 1**    Exit the current CTC session.

**Step 2**    Click the **Delete CTC Cache** button in the browser window (Figure 2-10 on page 2-24).

**Step 3**    Completely close the browser.

**Step 4**    Start the browser.

**Step 5**    Type the ONS 15454 SDH IP address and click **Go**. This can be the original IP address you logged on with or an IP address other than the original.

**Step 6**    Log into CTC. The browser will download the jar file from CTC.

✎
**Note**   The .jar files consist of core and element files. Core files are common to the ONS 15454 SDH, ONS 15454 SONET, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15454 SDH Release 1.0 uses a 3.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

# 2.4.8  Username or Password Does Not Match

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

Table 2-13 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-13   Username or Password Do Not Match*

| Possible Problem | Solution |
|---|---|
| The username or password entered do not match the information stored in the TCC-I. | 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 logon to the ONS 15454 SDH, type the *CISCO15* user name in capital letters and click **Login** (no password is required). |
| | See the "Verify Correct Username and Password" section on page 2-28. |

## Procedure: Verify Correct Username and Password

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

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

**Step 3**   Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Have Cisco TAC enter your system and create a new user name and password.

# 2.4.9  No IP Connectivity Exists Between Nodes

**Symptom**   The nodes have a grey icon and is usually accompanied by alarms.

Table 2-14 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-14    No IP Connectivity Exists Between Nodes*

| Possible Problem | Solution |
| --- | --- |
| A lost Ethernet connection. | Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "Ethernet Connections" section on page 2-30. |

## 2.4.10  DCC Connection Lost

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

Table 2-15 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-15    DCC Connection Lost*

| Possible Problem | Solution |
| --- | --- |
| A lost DCC connection. | Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "Clear the EOC Alarm" procedure on page 1-42. |

## 2.4.11  "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.

Table 2-16 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-16    "Path in Use" error when creating a circuit*

| Possible Problem | Solution |
| --- | --- |
| Another user has already selected the same source port to create another circuit. | 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 will get use of the port. The other user will get the "Path in Use" error. |
| | Cancel the circuit creation and start over, or click the **Back** button until you return to the initial circuit creation screen. The source port that was previously selected will no longer appear 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. |

## 2.4.12  Calculate and Design IP Subnets

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

Table 2-17 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-17    Calculate and Design IP Subnets*

| Possible Problem | Solution |
|---|---|
| The IP capabilities of the ONS 15454 SDH require specific calculations to properly design IP subnets. | Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 SDH IP capability, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*. |

## 2.4.13  Ethernet Connections

**Symptom**  Ethernet connections appear to be broken or are not working properly.

Table 2-18 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-18    Calculate and Design IP Subnets*

| Possible Problem | Solution |
|---|---|
| Improperly seated connections. | You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 2-11 when consulting the steps in the "Verify Ethernet Connections" section on page 2-31. |
| Incorrect connections. | |

*Figure 2-11    Ethernet connectivity reference*



Device "A"
192.168.1.25
255.255.255.0
VLAN #1 Member

Device "B"
192.168.1.75
255.255.255.0
VLAN #1 Member

Virtual
LAN # 1

ONS Node #1
Port #1 VLAN #1
Port #3 VLAN #1

ONS Node #2
Port #1 VLAN #1
Port #2 VLAN #1

Device "C"
192.168.1.50
255.255.255.0
VLAN #1 Member

Device "D"
192.168.1.100
255.255.255.0
VLAN #1 Member

32167
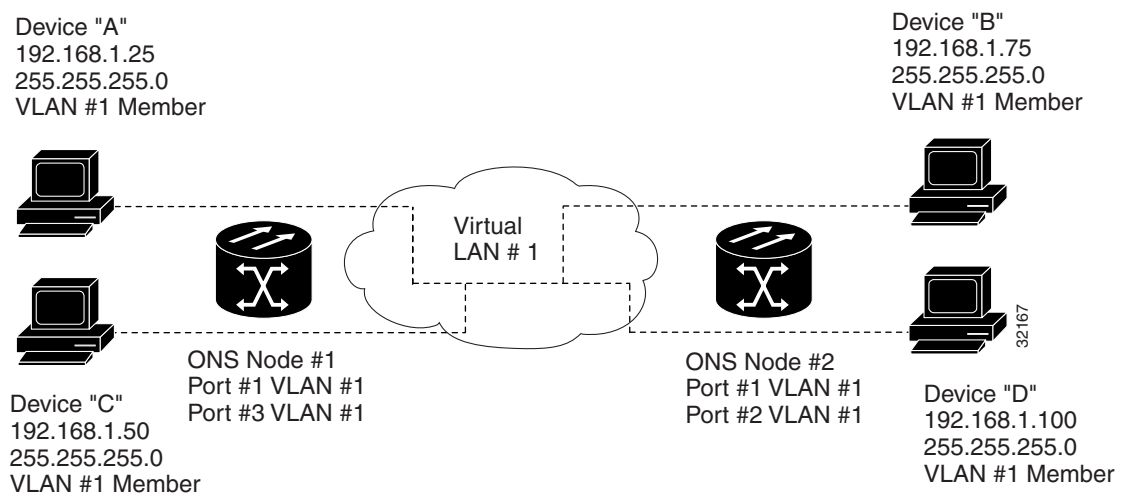
## Procedure: Verify Ethernet Connections

**Step 1**    Check for SONET alarms on the STS-N that carries the VLAN #1 Ethernet circuit. Clear any alarms by looking them up in Chapter 1, "Alarm Troubleshooting."

**Step 2**    Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 1, "Alarm Troubleshooting."

**Step 3**    Verify that the ACT LED on the Ethernet card is green.

**Step 4**    Verify that Ports 1 and 3 on ONS 15454 SDH #1 and Ports 1 and 2 on ONS 15454 SDH #2 have green link-integrity LEDs illuminated.

**Step 5**    If no green link-integrity LED is illuminated for any of these ports:

   **a.**    Verify physical connectivity between the ONS 15454 SDHs 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. Run the procedure in the "Lamp Test for Card LEDs" section on page 2-48.

**Step 6**    Verify connectivity between device A and device C by pinging between these locally attached devices (see the "Verify PC Connection to the ONS 15454 SDH (ping)" section on page 2-20). If the ping is unsuccessful:

   **a.**    Verify that device A and device C are on the same IP subnet.

   **b.**    Display the Ethernet card in CTC card view and click the **Provisioning > VLAN** tabs to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.

   **c.**    If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.

**Step 7**    Repeat Step 6 for devices B and D.

**Step 8**    Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 SDH #1 and ONS 15454 SDH #2 ports also use VLAN #1.

# 2.4.14  VLAN Cannot Connect to Network Device from Untag Port

**Symptom**  Networks that have a VLAN with one ONS 15454 SDH Ethernet card port set to Tagged and one ONS 15454 SDH Ethernet card set to Untag may have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 2-12). They may also see a higher than normal runt packets count at the network device attached to the Untag port.

*Figure 2-12   A VLAN with Ethernet ports at Tagged and Untag*
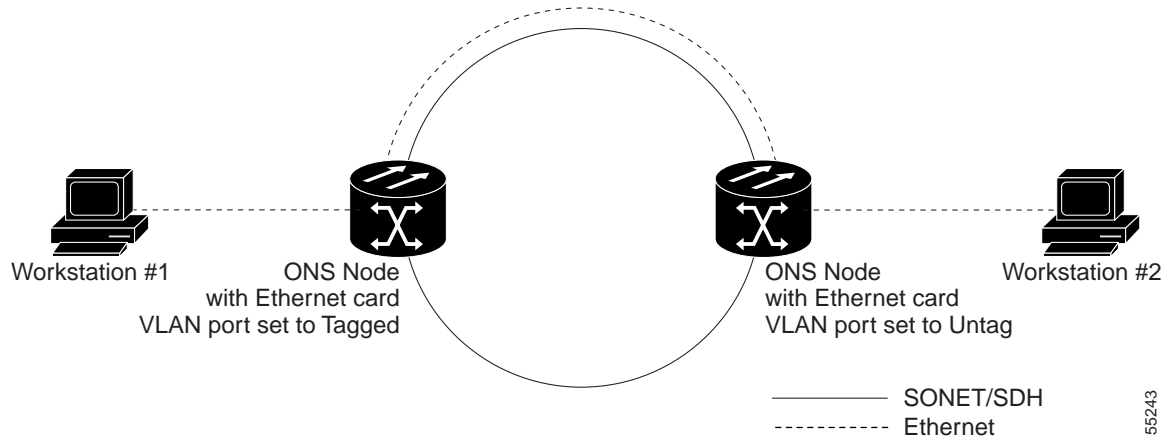


Table 2-19 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-19   Verify PC connection to ONS 15454 SDH (ping)*

| Possible Problem | Solution |
|---|---|
| The Tagged ONS 15454 SDH adds the 802.1Q tag and the Untag ONS 15454 SDH removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet. | 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 prevents the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with 802.1Q-compliant NIC cards will accept the tagged packets. Network devices with non-802.1Q compliant NIC cards will still drop these tagged packets. The solution may require upgrading network devices with non-802.1Q compliant NIC cards to 802.1Q-compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose 802.1Q compliance. |
| 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. | |

## Procedure: Change VLAN Port Tag and Untagged Settings

**Step 1**    Display the CTC card view for the Ethernet card involved in the problem VLAN.

**Step 2**    Click the **Provisioning > VLAN** tabs (Figure 2-13).

*Figure 2-13    Configuring VLAN membership for individual Ethernet ports*
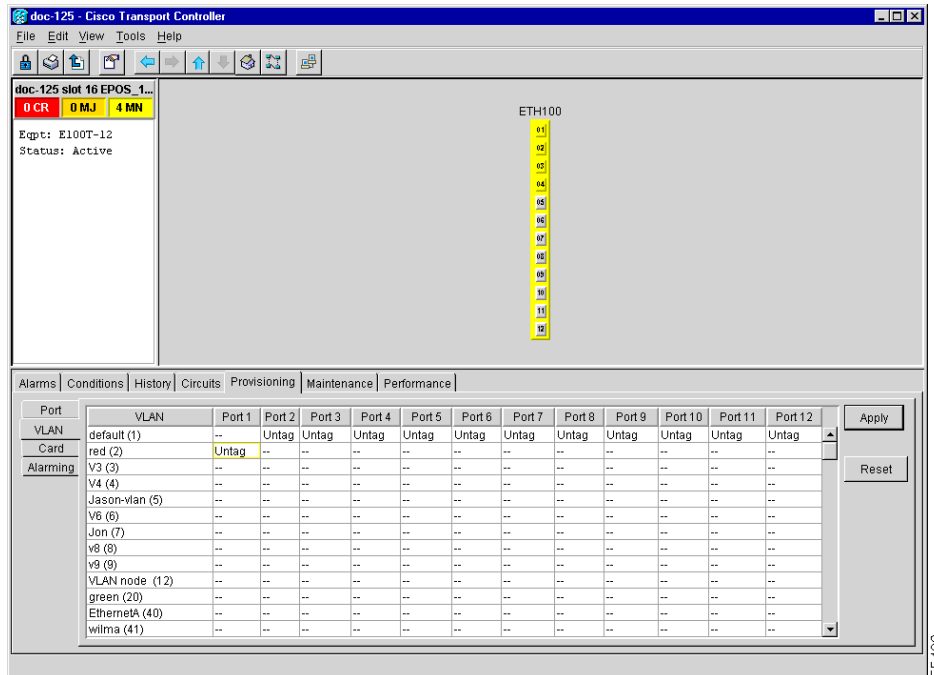


**Step 3**    If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.

**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**.

# 2.4.15  Cross-Connect Card Oscillator Fails

**Symptom:** The XC10G card can be affected by this problem. It is indicated by a CTNEQPT-PBPROT or CTNEQPT-PBWORK condition raised against all I/O cards in the node. The following conditions might also be raised on the node:

- SWMTXMOD against one or both cross-connect cards
- SDBER-EXCEED-LO against near-end or far-end line cards
- MS-AIS against far-end line cards

- LP-RFI against near-end line cards

Table 2-20 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-20   Cross-Connect Card Oscillator Fails*

| Possible Problem | Solution |
|---|---|
| The XC10G card has oscillator failure. | 1. If the Slot 8 cross-connect card is active, see the "Resolve the XC Oscillator Failure When Slot 8 XC Card is Active" section on page 2-34. |
| | 2. If the Slot 10 cross-connect card is active, see the "Resolve the XC Oscillator Failure When Slot 10 XC Card is Active" section on page 2-34. |

## Procedure: Resolve the XC Oscillator Failure When Slot 8 XC Card is Active

**Step 1** If the CTNEQPT-PBPROT condition is reported against all I/O cards in the node and the Slot 8 cross-connect card is active, right-click the Slot 10 cross-connect card.

**Step 2** Choose **Reset Card,** then click **OK**. (Slot 8 remains active and Slot 10 remains standby.)

**Step 3** If the alarm remains, reseat the Slot 10 card.

**Step 4** If CTNEQPT-PBPROT does not clear, replace the Slot 10 cross-connect card with a spare card.

**Step 5** If CTNEQPT-PBPROT does not clear, replace the spare card placed in Slot 10 with the original cross-connect card.

**Step 6** Right-click the Slot 8 card and choose **Reset Card**.

**Step 7** Click **OK** to activate the Slot 10 card and place the Slot 8 card in standby.

**Step 8** If you then see the CTNEQPT-PBWORK condition raised against all I/O cards in the node, verify that CTNEQPT-PBPROT has cleared on all I/O cards. Seeing CTNEQPT-PBWORK on the cards indicates that Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. Otherwise, go to Step 9.

**a.** Replace the Slot 8 cross-connect card with a spare card. (Slot 8 remains standby.)

**b.** Reseat the Slot 10 cross-connect card to activate the Slot 8 card and make Slot 10 standby.

**c.** Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

**Step 9** If you see CTNEQPT-PBPROT reported against all I/O cards in the node, this indicates that the Slot 10 card has a bad oscillator. If so, complete the following steps:

**a.** Replace the Slot 10 cross-connect card with a spare card. (The Slot 8 card is now active.)

**b.** Reseat the Slot 8 cross-connect card to make Slot 10 active.

**c.** Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

## Procedure: Resolve the XC Oscillator Failure When Slot 10 XC Card is Active

**Step 1** If the CTNEQPT-PBWORK condition is reported against all I/O cards in the node and the Slot 10 card is active, right-click the Slot 8 cross-connect card.

**Step 2** Choose **Reset Card** and click **OK**. (Slot 10 remains active and Slot 8 remains standby.)

**Step 3**  If the CTNEQPT-PBWORK condition does not clear, reseat the Slot 8 cross-connect card.

**Step 4**  If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.

**Step 5**  If the condition does not clear, replace the spare card placed in Slot 8 with the original cross-connect card.

**Step 6**  Right-click the Slot 10 cross-connect card.

**Step 7**  Choose **Reset Card** and click **OK**. The Slot 8 cross-connect card becomes active and Slot 10 becomes standby.

**Step 8**  If you have switched the Slot 8 card to active and continue to see CTNEQPT-PBWORK reported against all I/O cards in the node, this indicates the Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. If not, go to Step 9.

   **a.**  Replace the Slot 8 cross-connect card with a spare card. (The Slot 10 card is made active.)

   **b.**  Reseat the Slot 10 cross-connect card to make Slot 8 active.

   **c.**  Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

**Step 9**  If you then see the CTNEQPT-PBPROT condition raised against all I/O cards, verify that CTNEQPT-PBWORK has cleared on the I/O cards. This indicates that Slot 10 has a bad oscillator. If so, complete the following substeps:

   **a.**  Replace the Slot 10 cross-connect card with a spare card. (Slot 10 remains standby.)

   **b.**  Reseat the Slot 8 cross-connect card to activate the Slot 10 card and make Slot 8 standby.

   **c.**  Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

# 2.5  Circuits and Timing

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

## 2.5.1  Circuit Transitions to Partial State

**Symptom**  An automatic or manual transition of a circuit from one state to another state results in one of the following partial state conditions:

- **OOS_PARTIAL**  At least one of the connections in the circuit is in **OOS** state and at least one other connection in the circuit is in **IS**, **OOS_MT**, or **OOS_AINS** state.

- **OOS_MT_PARTIAL**  At least one connection in the circuit is in **OOS_MT** state and at least one other connection in the circuit is in **IS**, **OOS_MT**, or **OOS_AINS** state.

- **OOS_AINS_PARTIAL**  At least one connection in the circuit is in the **OOS_AINS** state and at least one other connection in the circuit is in **IS** or **OOS_AINS** state.

Table 2-21 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-21    Circuit in Partial State*

| Possible Problem | Solution |
|---|---|
| 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. | Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" section on page 2-36. Logon to the circuit node that did not change to the desired state and determine the version of software. If the software on the node is a version earlier than 3.4, 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 version 3.4, the partial state condition can be avoided by only using the circuit state(s) supported in the earlier software version. |
| During an automatic transition, some path-level defects and/or alarms were detected on the circuit. One end of the circuit is not properly terminated. | Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" section on page 2-36. Logon to the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state. |

## Procedure: View the State of Circuit Nodes

**Step 1**    Click the **Circuits** tab.

**Step 2**    From the Circuits tab list, select the circuit with the **\*_PARTIAL** state condition.

**Step 3**    Click the **Edit** button. The Edit Circuit window appears.

**Step 4**    In the Edit Circuit window, click the **State** tab.

The State tab window will list the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

# 2.5.2  TU-AIS on Unused VC Circuits

**Symptom**    An incomplete circuit path causes a tributary unit alarm indications signal (TU-AIS).

Table 2-22 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-22    TU-AIS on Unused VC Circuits*

| Possible Problem | Solution |
|---|---|
| The port on the reporting node is in-service but a node upstream on the circuit does not have an STM-N port in service. | A TU-AIS indicates that an upstream failure occurred at the virtual channel (VC) layer. TU-AIS alarms also occur on VC circuits that are not carrying traffic and on stranded bandwidth.<br><br>Perform the "Clear TU-AIS on Unused VC Circuits" section on page 2-37. |

## Procedure: Clear TU-AIS on Unused VC Circuits

**Step 1**      Determine the affected port.

**Step 2**      Record the node ID, slot number, port number, or VC number.

**Step 3**      Create a unidirectional VC circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VC11 cross connected to Source node/Slot 2/Port 2/VC11.

**Step 4**      Uncheck the bidirectional box in the circuit creation window.

**Step 5**      Give the unidirectional VC circuit an easily recognizable name, such as `delete me`.

**Step 6**      Display the DS3IN card in CTC card view. Click the **Maintenance > DS1** tabs.

**Step 7**      Locate the VC 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 2. Select the circuit and click **Delete**.

**Step 11**    Click **Yes** in the Delete Confirmation box.

**Step 12**    Display the DS3IN card in CTC card view. Click **Maintenance > DS1**.

**Step 13**    Locate the VC in Facility (line) Loopback.

**Step 14**    From the Loopback Type list, choose **None** and then click **Apply**.

**Step 15**    Click the **Alarm** tab and verify that the TU-AIS alarms have cleared.

**Step 16**    Repeat this procedure for all the TU-AIS alarms on the DS3IN cards.

## 2.5.3  Circuit Creation Error with VC Circuit

**Symptom**   You might 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 VC circuit in CTC.

Table 2-23 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-23   Circuit Creation Error with VC Circuit*

| Possible Problem | Solution |
|---|---|
| You may have run out of bandwidth on the VC cross-connect matrix at the ONS 15454 SDH indicated in the error message. | The matrix has a maximum capacity of 336 bidirectional VC cross-connects. Certain configurations will exhaust VC capacity with less than 336 bidirectional VCs in a MS-SPRing or less than 224 bidirectional VCs in SNCP or 1+1 protection. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide* for more information. |

## 2.5.4  ONS 15454 SDH Switches Timing Reference

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

Table 2-24 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-24   ONS 15454 SDH Switches Timing Reference*

| Possible Problem | Solution |
|---|---|
| The optical or SETS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source. | The ONS 15454 SDH internal clock operates at a Stratum 3 level of accuracy. This gives the ONS 15454 SDH a free-running synchronization accuracy of $\pm$ 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or $3.7\text{x}10^{-7}$/day, including temperature. |
| The optical or SETS input is not functioning. | ONS 15454 SDH free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source. |
| Sync Status Messaging (SSM) message is set to Don't Use for Sync (DUS). | |
| SSM indicates a Stratum 3 or lower clock quality. | |
| The input frequency is off by more than 15 ppm. | |
| The input clock wanders and has more than three slips in 30 seconds. | |
| A bad timing reference existed for at least two minutes. | |

## 2.5.5 Holdover Synchronization Alarm

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

Table 2-25 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-25    Holdover Synchronization Alarm*

| Possible Problem | Solution |
|---|---|
| The last reference input has failed. | 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" section on page 1-60 for a detailed description of this alarm. |

## 2.5.6 Free-Running Synchronization Mode

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

Table 2-26 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-26    Free-Running Synchronization Mode*

| Possible Problem | Solution |
|---|---|
| No reliable reference input is available. | The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" section on page 1-58 for a detailed description of this alarm. |

## 2.5.7 Daisy-Chained SETS Not Functioning

**Symptom**  You are unable to daisy-chain the SETS.

Table 2-27 outlines the problem that might cause this symptom and describes solutions to the problem.

*Table 2-27    Daisy-Chained SETS Not Functioning*

| Possible Problem | Solution |
|---|---|
| Daisy-chaining SETS is not supported on the ONS 15454 SDH. | Daisy-chaining SETS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the SETS clock and separately link them to each ONS 15454 SDH. |

# 2.6  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.

## 2.6.1  Bit Errors Appear for a Traffic Card

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

Table 2-28 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-28   Bit Errors Appear for a Line Card*

| Possible Problem | Solution |
|---|---|
| Faulty cabling or low optical-line levels. | 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 PJ (pointer justification) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454 SDH. Troubleshoot cabling problems using the "Network Troubleshooting Tests" section on page 2-1. Troubleshoot low optical levels using the "Faulty Fiber-Optic Connections" section on page 2-40. |

## 2.6.2  Faulty Fiber-Optic Connections

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

Table 2-29 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-29   Faulty Fiber-Optic Connections*

| Possible Problem | Solution |
|---|---|
| Faulty fiber-optic connections. | Faulty fiber-optic connections can be the source of SDH alarms and signal errors. Refer to the "Verify Fiber-Optic Connections" section on page 2-41. |
| Faulty gigabit interface connectors. | Faulty gigabit interface converters can be the source of SDH alarms and signal errors. Refer to the "Replace Faulty Gigabit Interface Converters" section on page 2-42. |
| Faulty Category 5 cables. | Faulty Category 5 cables can be the source of SDH alarms and signal errors. Refer to the "Crimp Replacement Category 5 Cables" section on page 2-44. |

**Warning**  **Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector. Class IIIb laser. Danger, laser radiation when open. The OC-192 laser is off when the safety key is off (labeled 0). 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. Avoid direct exposure to the beam. Invisible radiation is emitted from the aperture at the end of the fiber optic cable when connected, but not terminated.**

## Procedure: Verify Fiber-Optic Connections

**Step 1**    Ensure that a single-mode fiber connects to the ONS 15454 SDH STM-N card.

SM or SM fiber should be printed on the fiber span cable. ONS 15454 SDH STM-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 receive (Rx) end of the suspect fiber.

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

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

    **d.**    Verify the power meter is set to the appropriate wavelength for the optical card being tested (either 1310 nm or 1550 nm depending on the specific card).

    **e.**    Verify that the power level falls within the range specified for the card; see the "Optical Card Transmit and Receive Levels" section on page 2-46.

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

    **a.**    Clean or replace the fiber patch cords. If possible, do this for the STM-N card you are working on and the far-end card.

    **b.**    Clean the optical connectors on the card. If possible, do this for the STM-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 STM-N card to eliminate the possibility of a degrading transmitter on this STM-N card.

    **e.**    If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

       •    Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.

       •    Excessive number or fiber connectors; connectors take approximately 0.5 dB each.

       •    Excessive number of fiber splices; splices take approximately 0.5 dB each.

    ✎ **Note**    These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

**Step 5**   If no power level shows on the fiber, the fiber is bad or the transmitter on the optical card failed.

   **a.**   Check that the Transmit (Tx) and Receive (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. If possible, do this for the STM-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 optical card.

**Step 6**   If the power level on the fiber is above the range specified for the card, ensure that an ONS long-range (LR) card is not being used when an ONS intermediate-range (IR) card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter will be too powerful for the receiver on the receiving STM-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 STM-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS STM-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.

## Procedure: Replace Faulty Gigabit Interface Converters

Gigabit interface converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet port to link the port with the fiber-optic network. Cisco provides three GBIC models: one for short-reach applications, 15454E-GBIC-SX=, one for long-reach applications, 15454E-GBIC-LX=, and one for extra long-reach applications, 15454E-GBIC-ZX=. The short-reach, or "SX" model, connects to multimode fiber and has a maximum cabling distance of 1804 feet. The long-reach, or "LX" model, requires single-mode fiber and has a maximum cabling distance of 10000.5 metres (32,810 feet). The extra long-reach, or "ZX" model, supports extra long-reach applications on the 1550 nm wavelength for up to eighty kilometers. GBICs can be installed or removed while the card and shelf assembly are powered and running. GBIC transmit failure is characterized by a steadily blinking Fail LED on the Gigabit Ethernet (E1000-2/E1000-2-G) card. Figure 2-14 shows a GBIC.

*Figure 2-14   A gigabit interface converter (GBIC)*



Receiver   Transmitter

⚠️
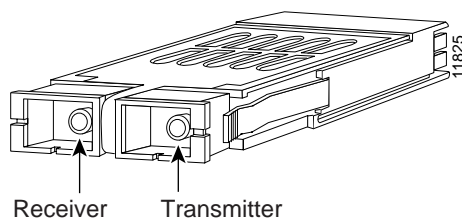
**Warning**      **Class 1 laser product**

⚠️

**Warning**      **Invisible laser radiation may be emitted from the aperture ports of single-mode fiber optic modules when a cable is not connected. Avoid exposure and do not stare into open apertures.**

**Step 1**    Disconnect the network interface fiber-optic cable from the GBIC SC connector and replace the protective plug.

**Step 2**    Release the GBIC from the card interface by simultaneously squeezing the two plastic tabs, one on each side of the GBIC.

**Step 3**    Slide the GBIC out of the Gigabit Ethernet front-panel slot.

✎

**Note**      A flap closes over the GBIC slot to protect the connector on the Gigabit Ethernet (E1000-2/E1000-2-G) card.

**Step 4**    Remove the new GBIC from its protective packaging.

**Step 5**    Check the part number to verify that the GBIC is the correct type for your network.

⚠️

**Caution**    Check the label on the GBIC carefully. The two GBIC models look similar.

**Step 6**    Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the front panel of the Gigabit Ethernet (E1000-2/E1000-2-G) card (see Figure 2-15 on page 2-44).

✎

**Note**      GBICs are keyed to prevent incorrect installation.

*Figure 2-15   Installing a GBIC on the E1000-2/E1000-2-G card*
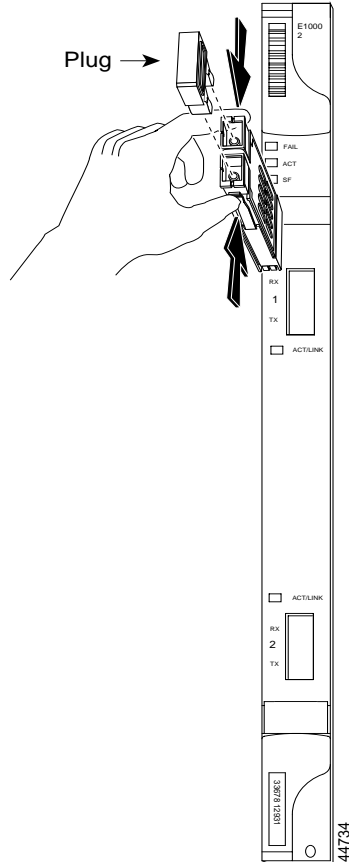


**Step 7**    Slide the GBIC through the front flap until you hear a click.

The click indicates that the GBIC is locked into the slot.

**Step 8**    When you are ready to attach the network interface fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

## Procedure: Crimp Replacement Category 5 Cables

You can crimp your own Category 5 cables for use with the ONS 15454 SDH. Use a cross-over cable when connecting an ONS 15454 SDH to a hub, LAN modem, or switch, and use a straight-through cable when connecting an ONS 15454 SDH to a router or workstation. Use Category 5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. shows the

Figure 2-16 on page 2-45 shows the RJ-45 connector pin numbering. Figure 2-17 on page 2-45 shows a straight-through cable wiring layout and Table 2-30 on page 2-45 shows the cable pinout. Figure 2-18 on page 2-46 shows a cross-over cable wiring layout and Table 2-31 on page 2-46 shows the cable pinout.

*Figure 2-16   RJ-45 pin numbers*



End view of RJ-45 plug                    Looking into an RJ-45 jack
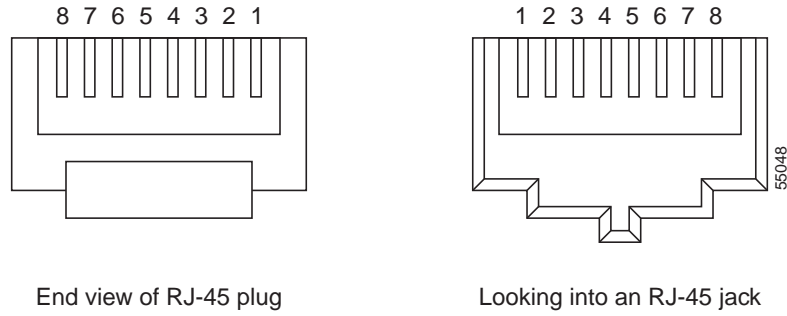
*Figure 2-17   A straight-through cable layout*
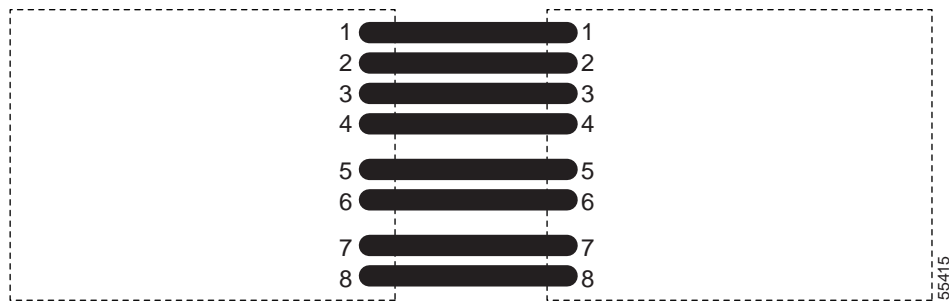


*Table 2-30   Straight-through cable pinout*

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

**Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4**

*Figure 2-18   A cross-over cable layout*
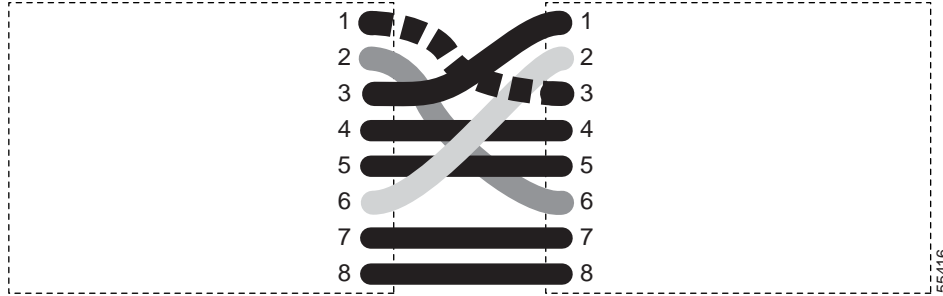


*Table 2-31   Cross-over cable pinout*

| 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.

## 2.6.3  Optical Card Transmit and Receive Levels

Each STM-N card has a transmit and receive connector on its faceplate. Table 2-32 shows the transmit and receive levels for the optical cards.

*Table 2-32   Optical Card Transmit and Receive Levels*

| Optical card | Rx | Tx |
|--------------|-----|-----|
| 4/STM1 LH 1310 | -8 to -28 dBm | -8 to -15 dBm |
| STM4 SH 1310 | -8 to -28 dBm | -8 to -15 dBm |
| STM4 LH 1310 | -8 to -28 dBm | +2 to -3 dBm |
| STM4 LH 1550 | -8 to -28 dBm | +2 to -3 dBm |
| STM16 SH 1310 | -8 to -28 dBm | +3 to -2 dBm |
| STM16 LH 1550 | -8 to -28 dBm | +3 to -2 dBm |
| STM16 EH 100GHz | -8 to -28 dBm | 0 to -2 dBm |
| STM64 LH 1550 | -9 to -17 dBm | +10 to +7 dBm |

# 2.7  Power and LED Tests

This section provides the "Power Supply Problems" section on page 2-47, the "Power Consumption for Node and Cards" section on page 2-48, and the "Lamp Test for Card LEDs" section on page 2-48.

## 2.7.1  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.

Table 2-33 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-33    Power Supply Problems*

| Possible Problem | Solution |
|---|---|
| Loss of power or low voltage.<br><br>Improperly connected power supply. | The ONS 15454 SDH requires a constant source of DC power to properly function. Input power is -48 VDC. Power requirements range from -42 VDC to -57 VDC.<br><br>A newly installed ONS 15454 SDH that is not properly connected to its power supply will not operate. Power problems can be confined to a specific ONS 15454 SDH or affect several pieces of equipment on the site.<br><br>A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 SDH to default to January 1, 1970, 00:04:15. For clock reset instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.<br><br>Refer to the "Isolate the Cause of Power Supply Problems" section on page 2-47. |

⚠

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

⚠

**Warning**    **When working with live power, always use proper tools and eye protection.**

⚠

**Warning**    **Always use the supplied electrostatic discharge (ESD) wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.**

## Procedure: Isolate the Cause of Power Supply Problems

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

   **a.**    Verify that the -48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane FMEC card under the clear plastic cover.

**b.** Verify that the power cable is #12 or #14 AWG and in good condition.

**c.** Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.

**d.** Verify that 20A 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 SDH FMEC card. 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 may affect power output.
- If brownouts occur, the power load and fuses may 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.

## 2.7.2  Power Consumption for Node and Cards

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

Table 2-34 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-34   Power Consumption for Node and Cards*

| Possible Problem | Solution |
|---|---|
| Improper power supply. | Refer to power information in the *Cisco ONS 15454 SDH Installation and Operations Guide*. |

## 2.7.3  Lamp Test for Card LEDs

**Symptom**   Card LED will not light or you are unsure if LEDs are working properly.

Table 2-35 describes the potential cause(s) of the symptom and the solution(s).

*Table 2-35    Lamp Test for Card LEDs*

| Possible Problem | Solution |
|---|---|
| Faulty LED | A lamp test verifies that all the card LEDs work. Run this diagnostic test as part of the initial ONS 15454 SDH turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order.<br><br>See the "Verify Card LED Operation" section on page 2-49. |

## Procedure: Verify Card LED Operation

**Step 1**    Click the **Maintenance > Diagnostic** tabs.

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

**Step 3**    Watch to make sure all the LEDs on the cards illuminate for several seconds.

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

If an LED does not illuminate, the LED is faulty. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

CHAPTER

**3**

# Card Reference

This chapter describes the Cisco ONS 15454 SDH cards. It includes descriptions, hardware specifications, and block diagrams for each card. For installation and card turn-up procedures, refer to Chapter 1 of the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4.*

## 3.1 Overview

The cards for the ONS 15454 SDH include Front Mount Electrical Connection cards (FMECs), common control cards, electrical cards, optical cards, and Ethernet cards. Each card is marked with a symbol that corresponds to a slot (or slots) on the ONS 15454 SDH shelf assembly. The cards are then installed into slots displaying the same symbols (refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4* for a list of slots/symbols). The overview in this section provides a summary of the cards.

### 3.1.1 Common Control Cards

Table 3-1 shows available common control cards for the ONS 15454 SDH.

*Table 3-1    Common Control Cards for the ONS 15454 SDH*

| Card | Description |
|------|-------------|
| TCC-I | The Timing Communications and Control–International (TCC-I) card is the main processing center of the ONS 15454 SDH and provides system initialization, provisioning, alarm reporting, maintenance, and diagnostics. |
| XC10G | The 10 Gigabit Cross Connect (XC10G) card is the central element for switching; it establishes connections and performs time-division switching (TDS). |
| AIC-I | The Alarm Interface Controller–International (AIC-I) card provides customer-defined alarm input/output (I/O), supports user data, and supports local and express orderwire. |

Power supply and alarming interfaces are dealt with in the Electrical Cards section of this chapter.

## 3.1.2 Electrical Cards

Table 3-2 shows available electrical cards for the ONS 15454 SDH.

*Table 3-2    Electrical Cards for the ONS 15454 SDH*

| Card | Description |
| --- | --- |
| E1-N-14 | The E1-N-14 card provides 14 E-1 ports and supports 1:0, 1:1, and 1:N protection. |
| E3-12 | The E3-12 card has 12 E-3 ports and supports 1:0 and 1:1 protection. |
| DS3i-N-12 | The DS3i-N-12 card has 12 DS-3 ports and supports 1:0, 1:1, and 1:N protection. |
| BLANK | The BLANK card assures fulfillment of EMC requirements in case of empty interface card slots. |
| FMEC-E1 | The FMEC-E1 card provides electrical connection into the system for 14 pairs of 75-ohm 1.0/2.3 miniature coax connectors for unbalanced E1 ports. |
| FMEC-E3/DS3 | The FMEC-E3/DS3 card provides electrical connection into the system for 12 pairs of 75-ohm 1.0/2.3 miniature coax connectors for unbalanced E3 or DS3 ports. |
| FMEC-DS1/E1 | The FMEC-DS1/E1 card provides electrical connection into the system for 14 pairs of 120-ohm balanced E1 ports; it uses high-density DB connectors. |
| FMEC-BLANK | The FMEC-BLANK card assures fulfillment of EMC requirements in case of empty FMEC slots. |
| MIC-A/P | The MIC-A/P card provides connection for one of the two redundant inputs of system power and system connection for input and output alarms. |
| MIC-C/T/P | The MIC-C/T/P card provides connection for one of the two redundant inputs of system power and system connection for LAN ports and system timing input/output. |

## 3.1.3 Optical Cards

Table 3-3 shows available optical cards for the ONS 15454 SDH.

*Table 3-3    Optical Cards for the ONS 15454 SDH*

| Card | Description |
| --- | --- |
| OC3 IR 4/STM1 SH 1310 | The OC3 IR 4/STM1 SH 1310 card provides four intermediate or short-range STM-1 ports and operates at 1310 nm. |
| OC12 IR/STM4 SH 1310 | The OC12 IR/STM4 SH 1310 card provides one intermediate or short-range STM-4 port and operates at 1310 nm. |
| OC12 LR/STM4 LH 1310 | The OC12 LR/STM4 LH 1310 card provides one long-range STM-4 port and operates at 1310 nm. |

*Table 3-3    Optical Cards for the ONS 15454 SDH  (continued)*

| Card | Description |
|------|-------------|
| OC12 LR/STM4 LH 1550 | The OC12 LR/STM4 LH 1550 card provides one long-range STM-4 port and operates at 1550 nm. |
| OC12 IR/STM4 SH 1310-4 | The OC12 IR/STM4 SH 1310-4 card provides four intermediate or short-range STM-4 ports and operates at 1310 nm. |
| OC48 IR/STM16 SH AS 1310 | The OC48 IR/STM16 SH AS 1310 card provides one intermediate or short-range STM-16 port at 1310 nm and operates in any multispeed or high-speed card slot. |
| OC48 LR/STM16 LH AS 1550 | The OC48 LR/STM16 LH AS 1550 card provides one long-range STM-16 port at 1550 nm and operates in any multispeed or high-speed card slot. |
| OC48 ELR/STM16 EH 100 GHz | The OC48 ELR/STM16 EH 100 GHz card provides one long-range (enhanced) STM-16 port and operates in any high-speed card slot. This card is available in 18 different wavelengths (9 in the Blue Band, 9 in the Red Band) in the 1550 nm range, every second wavelength in the ITU grid for 100-GHz spacing dense wavelength division multiplexing (DWDM). |
| OC192 LR/STM64 LH 1550 | The OC192 LR/STM64 LH 1550 card provides one long-range STM-64 port at 1550 nm and operates in any high-speed slot. |

## 3.1.4  Ethernet Cards

Table 3-4 shows available Ethernet cards for the ONS 15454 SDH. The Ethernet cards reduce the need for certain external Ethernet aggregation equipment such as hubs or switches.

*Table 3-4    Ethernet Cards for the ONS 15454 SDH*

| Card | Description |
|------|-------------|
| E100T-G | The E100T-G card provides twelve switched, auto-sensing, 10/100 Base-T Ethernet ports. |
| E1000-2-G | The E1000-2-G card provides two IEEE-compliant, 1000 MBit/s (Mbps) ports. Gigabit Interface Converters (GBICs) are separate. |
| G1000-4 | The G1000-4 card provides four IEEE-compliant, 1000 MBit/s (Mbps) ports. GBICs are separate. |

## 3.1.5  Card Power Consumption

Table 3-5 shows power consumption per card.

*Table 3-5    Card Power Consumption for the ONS 15454 SDH*

| Card | Watts | Amperage at –48V | Amperage at –40.5V | BTU/hr |
|------|-------|------------------|--------------------|--------|
| TCC-I | 21.00 | 0.44 | 0.52 | 71.7 |
| XC10G | 78.60 | 1.64 | 1.94 | 268.4 |
| AIC-I | 8 | 0.17 | 0.20 | 27.3 |
| E1N-14 | 12.60 | 0.26 | 0.31 | 43.0 |
| E3-12 | 44.00 | 0.92 | 1.09 | 150.2 |
| DS3i-N-12 | 30.00 | 0.63 | 0.74 | 102.4 |
| FMEC-E1 | 0.00 | 0.00 | 0.00 | 0.0 |
| FMEC-E3/DS3 | 0.00 | 0.00 | 0.00 | 0.0 |
| FMEC-DS1/E1 | 0.00 | 0.00 | 0.00 | 0.0 |
| MIC-A/P | (0.13) | via TCC-I | | |
| MIC-C/T/P | (0.38) | via TCC-I | | |
| OC3 IR 4/STM1 SH 1310 | 19.20 | 0.40 | 0.47 | 65.6 |
| OC12 IR/STM4 SH 1310 | 10.90 | 0.23 | 0.27 | 37.2 |
| OC12 LR/STM4 LH 1310 | 9.28 | 0.19 | 0.23 | 31.7 |
| OC12 LR/STM4 LH 1550 | 9.28 | 0.19 | 0.23 | 31.7 |
| OC12 LR/STM4 LH 1310-4 | 28 | 0.58 | 0.69 | 95.6 |
| OC48 IR/STM16 SH AS 1310 | 37.20 | 0.78 | 0.92 | 127.0 |
| OC48 LR/STM16 LH AS 1550 | 37.20 | 0.78 | 0.92 | 127.0 |
| OC48 ELR/STM16 EH 100 GHz | 31.20 | 0.65 | 0.77 | 106.5 |
| OC192 LR/STM64 LH 1550 | 72.20 | 1.50 | 1.78 | 246.5 |
| E100T-G | 65.00 | 1.35 | 1.60 | 221.9 |
| E1000-2-G | 53.50 | 1.11 | 1.32 | 182.7 |
| G1000-4 | 63 | 1.31 | 1.56 | 215.1 |
| Fan-Tray –48 VDC | 53 | 1.10 | 1.31 | 181.0 |

**Note** The ONS 15454 SDH is a flexible metro optical transport system supporting a wide variety of applications. The power consumption of the shelf assembly varies depending upon shelf configuration. Design your power distribution network based on your maximum ONS 15454 SDH system power draw, or the ONS 15454 SDH's maximum rated shelf power draw.

If you select to design your power plant to your maximum planned ONS 15454 SDH system configuration, the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4* lists the power consumption for each card that can be used to determine your maximum ONS 15454 SDH system power draw. The general guideline for fuse selection is 20% above the maximum calculated system power draw.

If you design your power system to the ONS 15454 SDH's maximum rated shelf power draw, Cisco

recommends that you select a power distribution system supporting a minimum capacity of 30A for each A and B power feeder on each ONS 15454 SDH shelf assembly. Feeder lines should be fused at 30A. This recommendation is based on the shelf assembly's current rated maximum power draw of 30A at –48 VDC. The maximum power draw configuration on the ONS 15454 SDH, based on the hardware available with Release 3.4, requires 30A at –48 VDC.

# 3.2  Electrical Card Protection

The ONS 15454 SDH provides a variety of electrical card protection methods. This section describes the protection options. Figure 3-1 on page 3-6 shows a 1:1 protection scheme and Figure 3-2 on page 3-7 shows a 1:N protection scheme.

## 3.2.1  1:0 Protection

The term 1:0 protection is sometimes used for an unprotected configuration.

## 3.2.2  1:1 Protection

In 1:1 protection, a working card is paired with a protect card of the same type. If the working card fails, the traffic from the working card switches to the protect card.When the failure on the working card is resolved, traffic automatically reverts to the working card. Figure 3-1 shows the ONS 15454 SDH in a 1:1 protection configuration; Slot 1 is protecting Slot 2, Slot 3 is protecting Slot 4, Slot 17 is protecting Slot 16, and Slot 15 is protecting Slot 14. Each working card is paired with a protect card. Slots 6 and 12 are not used for electrical cards. They have no corresponding FMEC slots.

*Figure 3-1    ONS 15454 SDH cards in a 1:1 protection configuration*
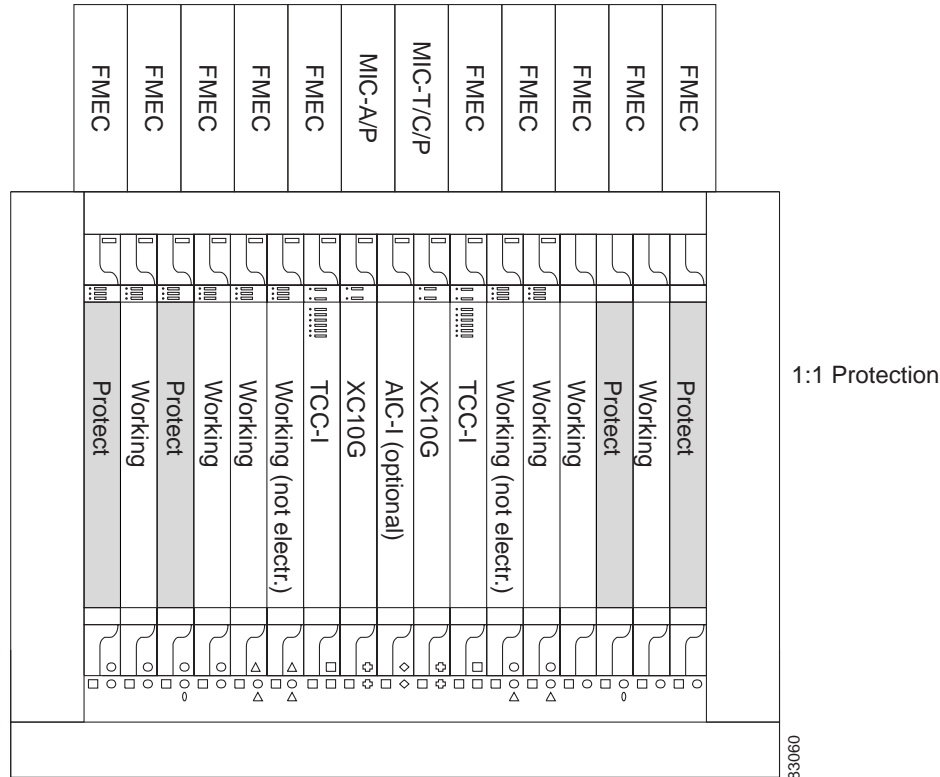


## 3.2.3  1:N Protection

1:N protection allows a single card to protect several working cards. An E1-N-14 card protects up to four E1-N-14 cards, and a DS3i-N-12 card protects up to four DS3i-N-12 cards.

Currently, 1:N protection operates only at the E-1 and DS-3 levels. The 1:N protect cards must match the levels of their working cards. For example, an E1-N-14 protects only E1-N-14 cards, and a DS3i-N-12 protects only DS3i-N-12 cards.

The physical E-1 or DS-3 ports on the ONS 15454 SDH FMEC cards use the working card until the working card fails. When the node detects this failure, the protection card takes over the physical E-1 or DS-3 electrical interfaces through the relays and signal bridging on the backplane. Figure 3-2 shows the ONS 15454 SDH in a 1:N protection configuration. Each side of the shelf assembly has only one card protecting all of the cards on that side.

**Figure 3-2    ONS 15454 SDH cards in a 1:N protection configuration**
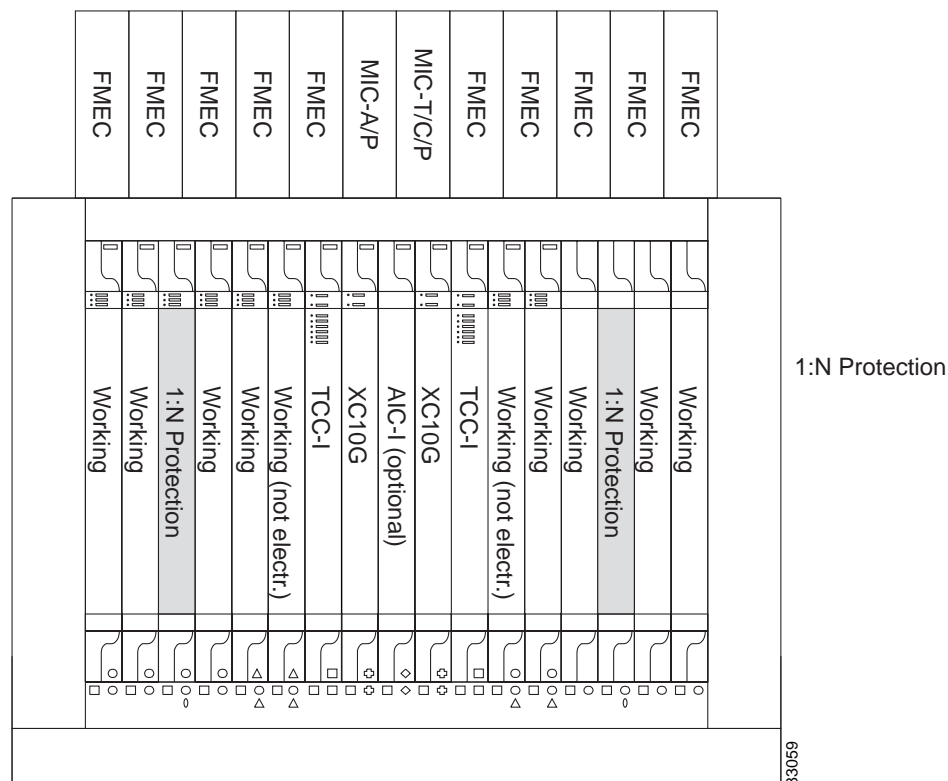


### 3.2.3.1  Revertive Switching

1:N protection supports revertive switching. Revertive switching sends the electrical interfaces back to the original working card after the card comes back online. Detecting an active working card triggers the reversion process. There is a variable time period for the lag between detection and reversion, called the revertive delay, which you can set using Cisco Transport Controller (CTC). For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4.* All cards in a protection group share the same reversion settings. 1:N protection groups default to automatic reversion.

### 3.2.3.2  1:N Protection Guidelines

Several rules apply to 1:N protection groups in the ONS 15454 SDH:

- Working and protect card groups must reside in the same card bank (A or B).
- The 1:N protect card must reside in Slot 3 for side A and Slot 15 for side B.
- Working cards might sit on either or both sides of the protect card.

The ONS 15454 SDH supports 1:N equipment protection for all add/drop multiplexer configurations (ring, linear, and terminal), as specified by ITU-T G.841.

The ONS 15454 SDH automatically detects and identifies a 1:N protection card when the card is installed in Slot 3 or Slot 15. However, the slot containing the 1:N card in a protection group must be manually provisioned as a protect slot because by default, all cards are working cards.

### 3.2.4 Electrical Card Protection and the FMECs

**Note**     For EIA descriptions and installation, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4.*

**Note**     When a protection switch moves traffic from the DS3i-N-12 working/active card to the DS3i-N-12 protect/standby card, ports on the new active/standby card cannot be taken out of service. Lost traffic can result when a port is taken out of service even if the DS3i-N-12 active/standby card no longer carries traffic.

# 3.3 Optical Card Protection

The ONS 15454 SDH currently supports 1+1 span protection to create redundancy for optical cards. Optical cards in any two slots can be paired for protection. 1+1 protection pairs a single working card with a single dedicated protect card. If the working card fails, the protect card takes over.

With non-revertive 1+1 protection, when a failure occurs and the signal switches from the working card to the protect card, the signal stays switched to the protect card until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working card when the working card comes back online.

# 3.4 Multiport Card Protection

For multiport cards such as the E1-N-14, the DS3i-N-12, and the OC3 IR 4/STM1 SH 1310, the ports on the protect card support the corresponding ports on the working card. With 1:1 or 1:N protection (electrical cards), the protect card must protect an entire slot. In other words, all the ports on the protect card will be used in the protection scheme.

With 1+1 protection (optical cards), protection can be assigned on a per-port basis. But the working and protect ports cannot be on the same card. In other words, any number of ports can be assigned as protection ports. On a four-port card, for example, you could assign one port as a protection port (protecting the corresponding port on the working card) and leave three ports unprotected. Conversely, you could assign three ports as protection ports and leave one port unprotected.

You create and modify protection schemes using CTC software. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4.*

# 3.5 Unprotected Cards (1:0 Protection)

Unprotected cards are not included in a protection scheme; therefore, a card failure or a signal error results in lost data. An unprotected configuration is sometimes called 1:0 protection. Because no bandwidth is reserved for protection, unprotected schemes maximize the available ONS 15454 SDH bandwidth. Figure 3-3 shows the ONS 15454 SDH in an unprotected configuration. All cards are in a working state.

*Figure 3-3    ONS 15454 SDH in an unprotected configuration*
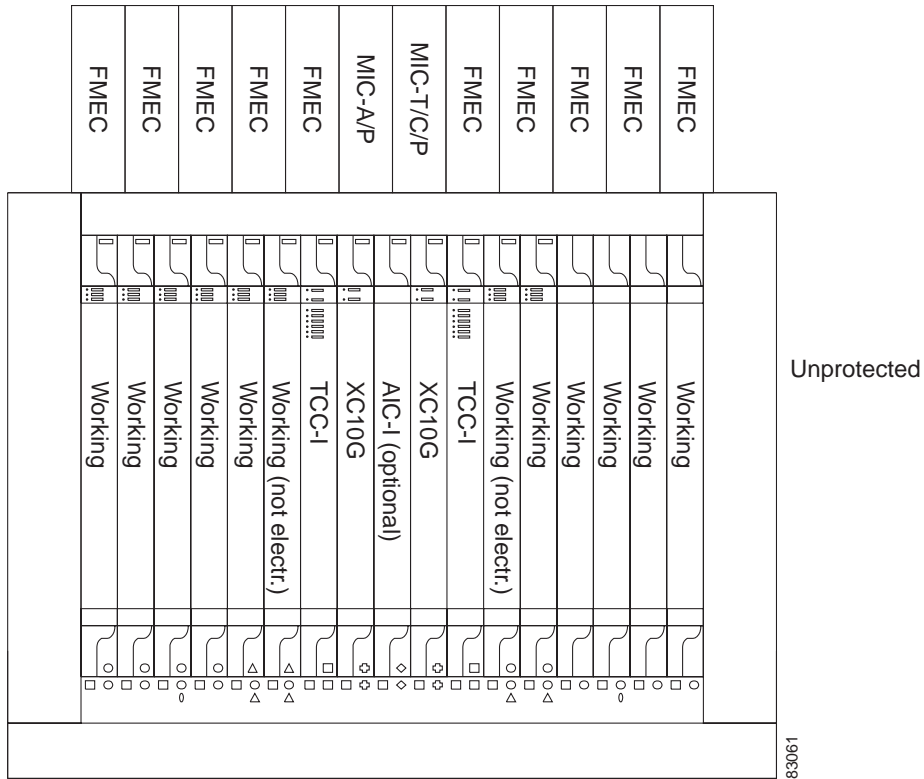


# 3.6  Timing Communications and Control–International (TCC-I) Card

The TCC-I performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SDH section overhead (SOH) data communications channel (DCC) termination, and system fault detection for the ONS 15454 SDH. The TCC-I also ensures that the system maintains Stratum 3E (G.813) timing requirements. Figure 3-4 on page 3-10 shows the TCC-I faceplate and Figure 3-5 on page 3-11 shows a block diagram of the card.

*Figure 3-4    TCC-I faceplate*
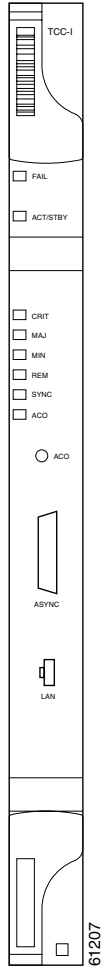
*Figure 3-5    TCC-I block diagram*
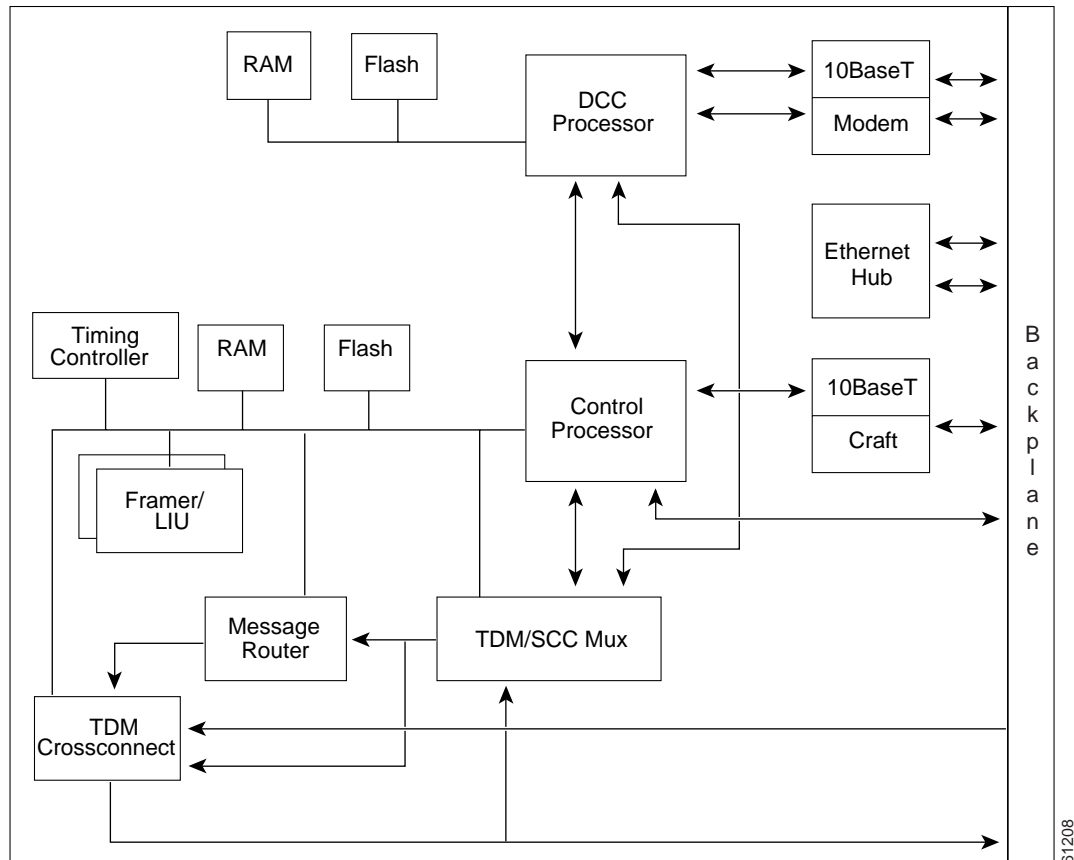


## 3.6.1  TCC-I Functionality

The TCC-I supports multichannel, high-level data link control (HDLC) processing for the DCC. Up to 48 DCCs can be routed over the TCC-I and up to ten DCCs can be terminated at the TCC-I (subject to available optical digital communication channels). The TCC-I selects and processes ten DCCs to facilitate remote system management interfaces.

The TCC-I also originates and terminates a cell bus carried over the module. The cell bus supports links between any two cards in the node, which is essential for peer-to-peer communication. Peer-to-peer communication accelerates protection switching for redundant cards.

The node database, IP address, and system software are stored in TCC-I non-volatile memory, which allows quick recovery in the event of a power or card failure.

The TCC-I performs all system-timing functions for each ONS 15454 SDH. The TCC-I monitors the recovered clocks from each traffic card and two building integrated timing supply (BITS) ports for frequency accuracy. The TCC-I selects a recovered clock, a BITS or an internal Stratum 3E reference as the system-timing reference. You can provision any of the clock inputs as primary or secondary timing sources. A slow-reference tracking loop allows the TCC-I to synchronize with the recovered clock, which provides holdover if the reference is lost.

Install TCC-I cards in Slots 7 and 11 for redundancy. If the active TCC-I fails, traffic switches to the protect TCC-I. All TCC-I protection switches conform to protection switching standards when the bit error rate (BER) counts are not in excess of 1 * 10 exp – 3 and completion time is less than 50 ms.

The TCC-I uses a 10Base-T LAN port for user interfaces, led via the backplane to the port accessible on the front of the MIC-C/T/P FMEC.

**Note**    Cisco does not support operation of the ONS 15454 SDH with only one TCC-I card. For full functionality and to safeguard your system, always operate in a redundant configuration.

**Note**    CTC software does not monitor for the presence or absence of FMECs unless the TCC-I card(s) have reached the active/standby state. During transitional states such as power-up or TCC-I reset, CTC ignores the FMEC inventory displayed in node view.

**Note**    When a second TCC-I card is inserted into a node, it synchronizes its software, its backup software, and its database with the active TCC-I. If the software version of the new TCC-I does not match the version on the active TCC-I, the newly inserted TCC-I copies from the active TCC-I, taking about 15 to 20 minutes to complete. If the backup software version on the new TCC-I does not match the version on the active TCC-I, the newly inserted TCC-I copies the backup software from the active TCC-I again, taking about 15 to 20 minutes. Copying the database from the active TCC-I takes about 3 minutes. Depending on the software version and backup version the new TCC-I started with, the entire process can take between 3 and 40 minutes.

## 3.6.2  TCC-I Card-Level Indicators

The TCC-I faceplate has eight LEDs. The first two LEDs are card-level indicators. These indicators are described in Table 3-6.

*Table 3-6    TCC-I Card-Level Indicators*

| Card-Level LEDs | Definition |
| --- | --- |
| Red FAIL LED | This LED is lit during reset. The FAIL LED flashes during the boot and write process. Replace the unit if the FAIL LED persists. |
| ACT/STBY LED<br><br>Green (Active)<br><br>Yellow (Standby) | The ACT/STBY (Active/Standby) LED indicates the TCC-I is active (green) or in standby (yellow) mode. The ACT/STBY LED also provides the timing reference and shelf control. When the TCC-I is writing to the Active or Standby TCC-I, its Active or Standby LED blinks. To avoid memory corruption, do not remove the TCC-I when the Active or Standby LED is blinking. |

## 3.6.3  Network-Level Indicators

The TCC-I faceplate has eight LEDs. Six LEDs are network-level indicators. These indicators are described in Table 3-7.

*Table 3-7    TCC-I System-Level Indicators*

| System-Level LEDs | Definition |
|---|---|
| Red CRIT LED | Used to indicate critical alarms in the network at the local terminal. |
| Red MAJ LED | Used to indicate major alarms in the network at the local terminal. |
| Yellow MIN LED | Used to indicate a minor alarm in the network at the local terminal. |
| Red REM LED | Provides first-level alarm isolation. The remote (REM) LED turns red when an alarm is present in one or several of the remote terminals. |
| Green SYNC LED | Used to indicate that node timing is synchronized to an external reference. |
| Green ACO LED | After pressing the alarm cutoff (ACO) button, the green ACO LED illuminates. The ACO button opens the audible closure on the backplane. ACO state is stopped if a new alarm occurs. After the originating alarm is extinguished, the ACO LED and audible alarm control are reset. |

# 3.6.4 TCC-I Specifications

- CTC Software
    - Interface: 10 Base-T LAN (via backplane)
    - Access: On the MIC-A/P unit
- Synchronization
    - Stratum 3E, per ITU-T G.813
    - Free running access: Accuracy $\neq -4.6$ ppm
    - Holdover Stability: 3.7 * 10 exp – 7 per day including temperature (< 255 slips in first 24 hours)
    - Reference: External BITS, line, internal
- Environmental
    - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
    - Operating humidity: 5 to 95%, noncondensing
    - Power consumption: 9.82W, 0.20A at –48V, 33.5 BTU/hr
- Dimensions
    - Height: 321.3 mm (12.650 in.)
    - Width: 18.2 mm (0.716 in.)
    - Depth: 228.6 mm (9.000 in.)
    - Depth with backplane connector: 235 mm (9.250 in.)
    - Weight not including clam shell: 0.7 kg (1.5 lb)
- Compliance

    ONS 15454 SDH cards, when installed in a system, comply with these standards:
    - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.7  Cross Connect XC10G Card

The XC10G card cross connects STM-1, STM-4, STM-16, and STM-64 signal rates. The XC10G provides a maximum of 384 x 384 VC-4 non-blocking cross connections. Any STM-1 on any port can be connected to any other port, meaning that the STM cross-connections are non-blocking.

The XC10G faceplate, cross-connects, and a block diagram are shown in Figure 3-6, Figure 3-7, and Figure 3-8.

**Note**    The lowest level cross-connect is STM-1. Lower level signals, such as E-1, DS-3, or E-3, can be dropped. This might leave part of the bandwidth unused.

*Figure 3-6    XC10G faceplate*
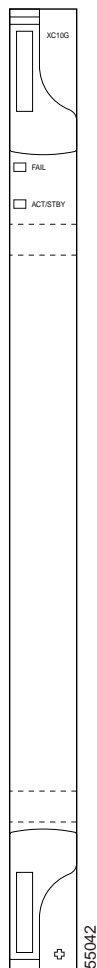
*Figure 3-7    XC10G Cross-Connect matrix*
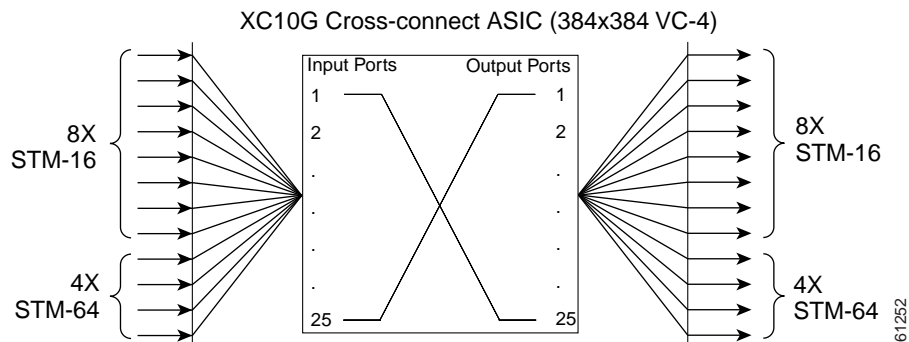


*Figure 3-8    XC10G block diagram*
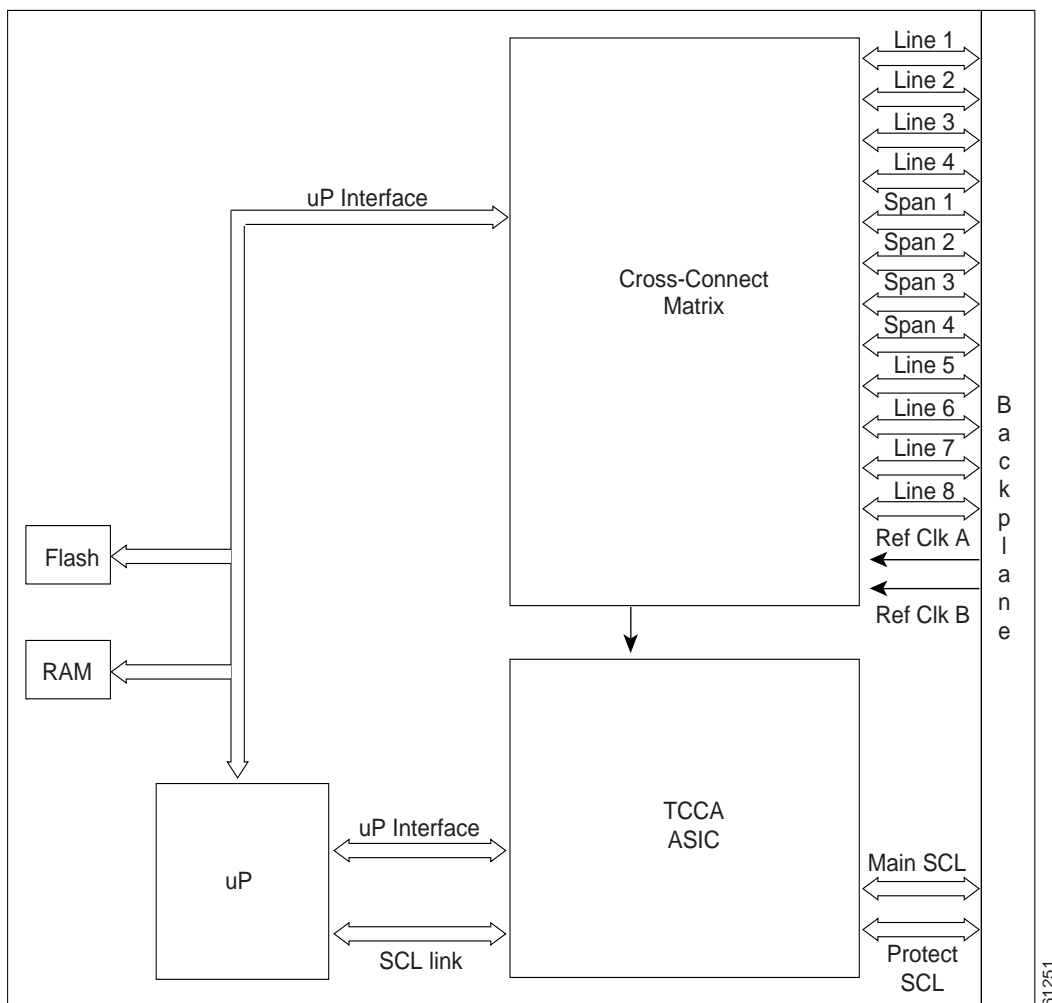


The XC10G card manages up to 192 bidirectional STM-1 cross-connects. The TCC-I assigns bandwidth to each slot on a per STM-1 basis. The XC10G card works with the TCC-I card to maintain connections and set up cross-connects within the system. The XC10G is required to operate the ONS 15454 SDH.

You can establish cross-connect and provisioning information through the Cisco Transport Controller (CTC). The TCC-I establishes the proper internal cross-connect information and sends the setup information to the XC10G cross-connect card.

**Note**    Cisco does not recommend nor support operating the ONS 15454 SDH with only one XC10G card. To safeguard your system, always operate in a redundant configuration.

## 3.7.1  XC10G Card-Level Indicators

The XC10G faceplate has two card-level LEDs, described in Table 3-8.

*Table 3-8    XC10G Card-Level Indicators*

| Card-Level LEDs | Definition |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the unit if the red FAIL LED persists. |
| ACT/STBY LED<br><br>Green (Active)<br><br>Yellow (Standby) | The ACT/STBY (Active/Standby) LED indicates whether the XC10G is active and carrying traffic (green) or in standby mode to the active XC10G card (yellow). |

## 3.7.2  XC10G Card Specifications

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 85%, noncondensing
  - Power consumption: 78.60W, 1.64A at –48V, 268.4 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.6 kg (1.5 lb)
- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.8  Alarm Interface Controller–International Card

The optional Alarm Interface Controller–International (AIC-I) card provides customer-defined alarm I/O, and supports user data and local and express orderwire. It provides 16 customer-defined input contacts and 4 customer-defined input/output contacts. It requires the MIC-A/P for connection to the alarm contacts. Figure 3-9 shows the AIC-I faceplate and a block diagram of the card.

*Figure 3-9    AIC-I faceplate and block diagram*
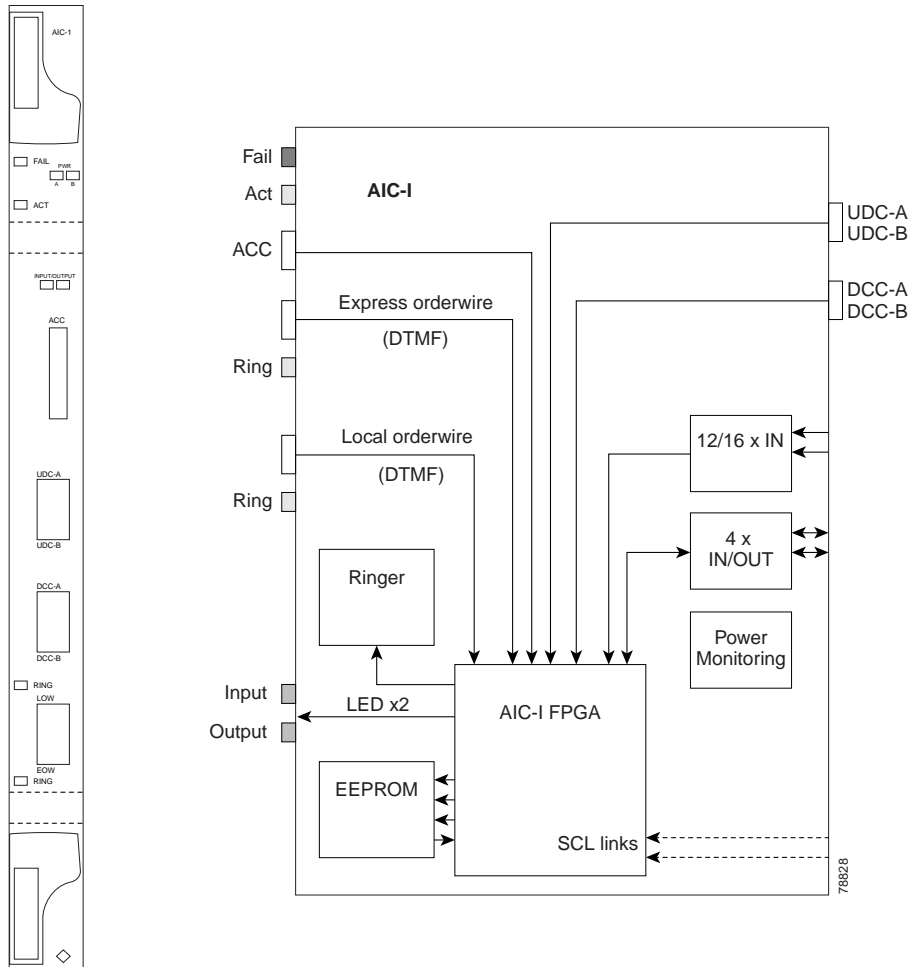
## 3.8.1  AIC-I Card-Level Indicators

The AIC-I card has eight card-level LED indicators, described in Table 3-9.

*Table 3-9     AIC-I Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| Green ACT LED | The green ACT LED indicates that the AIC-I card is provisioned for operation. |
| Green/red PWR A LED | The PWR A LED is green when a supply voltage within the specified range has been sensed on supply input A. It is red when the input voltage on supply input A is out of range. |
| Green/red PWR B LED | The PWR B LED is green when a supply voltage within the specified range has been sensed on supply input B. It is red when the input voltage on supply input B is out of range. |
| Yellow INPUT LED | The INPUT LED is yellow when there is an alarm condition on at least one of the alarm inputs. |
| Yellow OUTPUT LED | The OUTPUT LED is yellow when there is an alarm condition on at least one of the alarm outputs. |
| Green RING LED | The green RING LED on the local orderwire (LOW) side is flashing when a call is received on the LOW. |
| Green RING LED | The green RING LED on the express orderwire (EOW) side is flashing when a call is received on the EOW. |

## 3.8.2  User-Defined Alarms

The AIC-I card provides input/output alarm contact closures. You can define up to sixteen external alarm inputs and four external alarm inputs/outputs (user configurable). The physical connections are made using the MIC-A/P. The alarms are defined using CTC. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4*.

LEDs on the front panel of the AIC-I indicate the status of the alarm lines: one LED representing all the inputs and one LED representing all the outputs. External alarms (input contacts) are typically used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions. External controls (output contacts) are typically used to drive visual or audible devices such as bells and lights, but they can control other devices such as generators, heaters, and fans.

You can program each of the sixteen input alarm contacts separately. Choices include Alarm on Closure or Alarm on Open, an alarm severity of any level (Critical, Major, Minor, Not Alarmed, Not Reported), and Service Affecting or Non-Service Affecting alarm-service level, and a 63-character alarm description for CTC display in the alarm log. You cannot assign the fan-tray abbreviation for the alarm; the abbreviation reflects the generic name of the input contacts. The alarm condition remains raised until the external input stops driving the contact or you de-provision the alarm input.

The output contacts can be provisioned to close on a trigger or to close manually. The trigger can be a local alarm severity threshold, a remote alarm severity, or a virtual wire, as follows:

- Local NE alarm severity: A hierarchy of non-reported, non-alarmed, minor, major, or critical alarm severities that you set to cause output closure. For example, if the trigger is set to minor, a minor alarm or above is the trigger.

- Remote NE alarm severity: Same as the Local NE alarm severity but applies to remote alarms only.

- Virtual wire entities: You can provision any environmental alarm input to raise a signal on any virtual wire on external outputs 1 through 4 when the alarm input is an event. You can provision a signal on any virtual wire as a trigger for an external control output.

You can also program the output alarm contacts (external controls) separately. In addition to provisionable triggers, you can manually force each external output contact to open or close. Manual operation takes precedence over any provisioned triggers that might be present.

# 3.8.3 Orderwire

Orderwire allows a craftsperson to plug a phoneset into an ONS 15454 SDH and communicate with craftspeople working at other ONS 15454 SDHs or other facility equipment. The orderwire is a pulse code modulation (PCM) encoded voice channel that uses E1 or E2 bytes in the multiplex section overhead and in the regenerator section overhead.

The AIC-I allows simultaneous use of both local (section overhead signal) and express (line overhead channel) orderwire channels on an SDH ring or particular optics facility. Express orderwire also allows communication via regeneration sites when the regenerator is not a Cisco device.

You can provision orderwire functions with CTC similar to the current provisioning model for DCC channels. In CTC, you provision the orderwire communications network during ring turn-up so that all NEs on the ring can reach one another. Orderwire terminations (i.e., the optics facilities that receive and process the orderwire channels) are provisionable. Both express and local orderwire can be configured as on or off on a particular SDH facility. The ONS 15454 SDH supports up to four orderwire channel terminations per shelf. This allows linear, single ring, dual ring, and small hub-and-spoke configurations. Keep in mind that orderwire is not protected in ring topologies such as multiplex section-shared protection ring (MS-SPRing) and subnetwork connection protection (SNCP).

⚠️
**Caution**    Do not configure orderwire loops. Orderwire loops cause feedback that disables the orderwire channel.

The ONS 15454 SDH implementation of both local and express orderwire is broadcast in nature. The line acts as a party line. Anyone who picks up the orderwire channel can communicate with all other participants on the connected orderwire subnetwork. The local orderwire party line is separate from the express orderwire party line. Up to four OC-N/STM-N facilities for each local and express orderwire are provisionable as orderwire paths.

✎
**Note**    The OC3 IR 4/STM1 SH 1310 card does not support the EOW channel.

The AIC-I supports selective dual tone multifrequency (DTMF) dialing for telephony connectivity which causes specific or all ONS 15454 SDH AIC-Is on the orderwire subnetwork to "ring." The ringer/buzzer resides on the AIC-I. There is also a "ring" LED that mimics the AIC-I ringer. It flashes when a call is received on the orderwire subnetwork. A party line call is initiated by pressing **\*0000** on the DTMF pad. Individual dialing is initiated by pressing **\*** and the individual four-digit number on the DTMF pad.

The orderwire ports are standard RJ-11 receptacles. The pins on the orderwire ports correspond to the tip and ring orderwire assignments. Orderwire pin assignments are described in Table 3-10. Figure 3-10 on page 3-20 shows the RJ-11 cable.

*Table 3-10    Orderwire Pin Assignments*

| RJ-11 Pin Number | Description |
| --- | --- |
| 1 | Four-wire receive ring |
| 2 | Four-wire transmit tip |
| 3 | Two-wire ring |
| 4 | Two-wire tip |
| 5 | Four-wire transmit ring |
| 6 | Four-wire receive tip |

*Figure 3-10    RJ-11 cable connector*
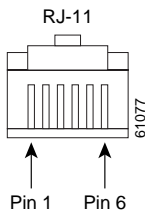


When provisioning the orderwire subnetwork, make sure that an orderwire loop does not exist. Loops cause oscillation and an unusable orderwire channel.

## 3.8.4  User Data Channel

The User Data Channel (UDC) features a dedicated data channel of 64 kBit/s (kbps) (F1 byte) between two nodes in an ONS 15454 SDH network. Each AIC-I card provides two UDCs, UDC-A and UDC-B, through separate RJ-11 connectors on the front of the AIC-I. Each UDC can be routed to an individual optical interface in the ONS 15454 SDH system. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4*.

The UDC ports are standard RJ-11 receptacles. The UDC pin assignments are listed in Table 3-11. Figure 3-10 shows the RJ-11 cable connector.

*Table 3-11    UDC Pin Assignments*

| RJ-11 Pin Number | Description |
| --- | --- |
| 1 | For future use |
| 2 | TXN |
| 3 | RXN |
| 4 | RXP |
| 5 | TXP |
| 6 | For future use |

## 3.8.5 Data Communication Channel

The Data Communication Channel (DCC) features a dedicated data channel of 576 kBit/s (kbps) (D4 to D12 bytes) between two nodes in an ONS 15454 SDH network. Each AIC-I card provides two DCCs, DCC-A and DCC-B, through separate RJ-45 connectors on the front of the AIC-I. Each DCC can be routed to an individual optical interface in the ONS 15454 SDH system. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4.*

**Note**   DCC connection cannot be provisioned if DCC tunneling is configured on this span.

The DCC ports are standard RJ-45 receptacles. The DCC pin assignments are described in Table 3-12.

*Table 3-12    DCC Pin Assignments*

| RJ-45 Pin Number | Description |
| --- | --- |
| 1 | TCLKP |
| 2 | TCLKN |
| 3 | TXP |
| 4 | TXN |
| 5 | RCLKP |
| 6 | RCLKN |
| 7 | RXP |
| 8 | RXN |

## 3.8.6 AIC-I Specifications

- Alarm Inputs
    - Number of inputs: 16
    - Opto-coupler isolated
    - Label customer provisionable
    - Severity customer provisionable
    - Common 32V output for all alarm-inputs
    - Each input limited to 2 mA
    - Termination: Via MIC-A/P
- Alarm Outputs
    - Number of outputs: 4 (user configurable as inputs)
    - Switched by opto-MOS (metal oxide semiconductor)
    - Triggered by definable alarm condition
    - Maximum allowed open circuit voltage: 60 VDC
    - Maximum allowed closed circuit current: 100 mA
    - Termination via MIC-A/P

- EOW/LOW

  – ITU-T G.711, ITU-T G.712, Telcordia GR-253-CORE

  – A-law, mu-law

✎
**Note**    Due to the nature of mixed coding, in a mixed-mode configuration (A-law/mu-law) the orderwire is not ITU-T G.712 compliant.

  – Orderwire party line

  – DTMF signaling

- UDC

  – Bit rate: 64 kBit/s (kbps), co-directional

  – ITU-T G.703

  – Input/output impedance: 120 ohms

  – Termination: RJ-11 connectors

- DCC

  – Bit rate: 576 kBit/s (kbps)

  – RS-485/V11

  – Input/output impedance: 120 ohms

  – Termination: RJ-45 connectors

- ACC connection for additional alarm interfaces

  – For future use

- Environmental

  – Operating temperature: –40 to +65 degrees Celsius (–40 to +149 degrees Fahrenheit)

  – Operating humidity: 5 to 95%, noncondensing

  – Power consumption: 8.00W, 0.17A, 27.3 BTU/Hr.

- Dimensions

  – Height: 321.3 mm (12.650 in.)

  – Width: 18.2 mm (0.716 in.)

  – Depth: 228.6 mm (9.000 in.)

  – Card Weight: 1.8 lb (0.82 kg)

- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:

  – Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

## 3.9  E1-N-14 Card

The fourteen-port ONS 15454 SDH E1-N-14 card provides fourteen ITU-compliant, G.703 E-1 ports. Each port of the E1-N-14 card operates at 2.048 MBit/s (Mbps) over a 120-ohm, twisted-pair copper cable (with FMEC-DS1/E1) or over a 75-ohm unbalanced coaxial cable (with FMEC-E1). Figure 3-11 shows the E1-N-14 faceplate and Figure 3-12 on page 3-24 shows a block diagram of the card.

*Figure 3-11    E1-N-14 faceplate*
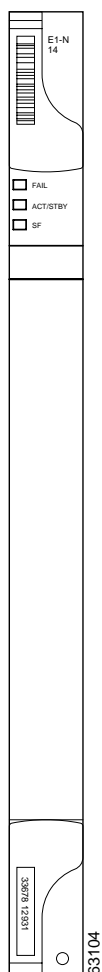
*Figure 3-12   E1-N-14 block diagram*
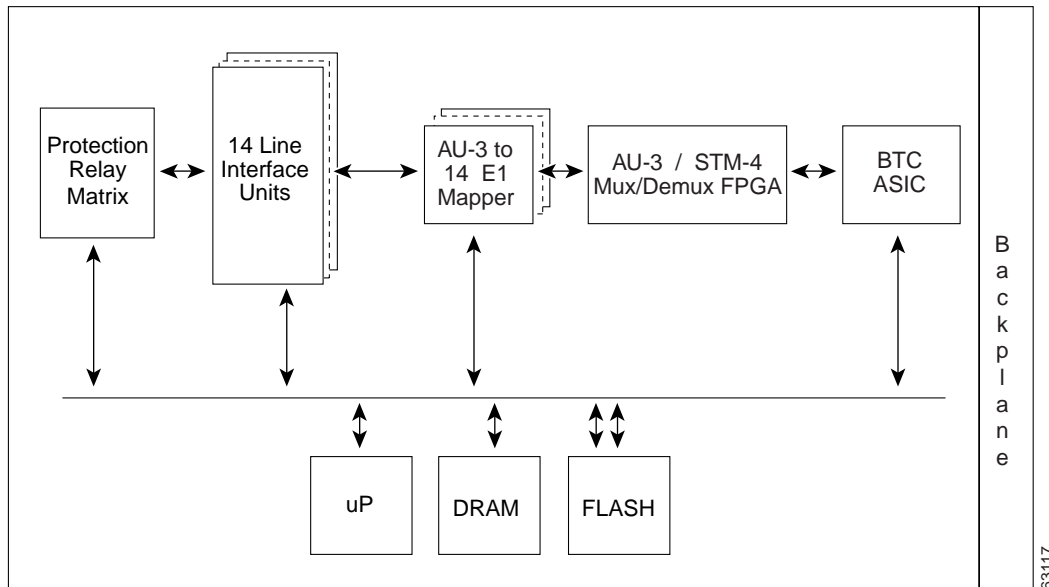


Each E1-N-14 port features ITU-T G.703 compliant outputs and inputs supporting cable losses of up to 6 dB at 1024 kHz. The E1-N-14 card supports 1:N (N <= 4) protection. You can also provision the E1-N-14 to monitor line and frame errors in both directions.

The E1-N-14 card can function as a working or protect card in 1:1 or 1:N protection schemes. If you use the E1-N-14 as a standard E-1 card in a 1:1 protection group, you can install the E1-N-14 card in any multispeed or high-speed card slot on the ONS 15454 SDH. If you use the card's 1:N functionality, you must install an E1-N-14 card in Slot 3 (for bank A) or Slot 15 (for bank B).

You can group and map E1-N-14 card traffic in VC-12 as per ITU-T G.707 to any other card in an ONS 15454 SDH node. For performance-monitoring purposes, you can gather bidirectional E-1 frame-level information (for example, loss of frame, parity errors, or CRC errors).

**Note**   The lowest level cross-connect is STM-1. Lower level signals, such as E-1, DS-3, or E-3, can be dropped. This might leave part of the bandwidth unused.

## 3.9.1  E1-N-14 Card-Level Indicators

The E1-N-14 card faceplate has three LEDs, described in Table 3-13.

*Table 3-13    E1-N-14 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the FAIL LED persists. |
| ACT/STBY LED<br><br>Green (Active)<br><br>Yellow (Standby) | The ACT/STBY LED indicates when the E1-N-14 card is operational and ready to carry traffic (green) or when the card is in standby mode (yellow). |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, or high BERs on one or more of the card's ports. |

## 3.9.2  E1-N-14 Port-Level Indicators

You can obtain the status of the fourteen E-1 ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.9.3  E1-N-14 Specifications

- E1-N-14 Input
    - Bit rate: 2.048 MBit/s (Mbps) +/– 50 ppm
    - Frame format: Unframed, ITU-T G.704 framed
    - Line code: HDB-3
    - Termination: Via FMEC-E1 (for 75 ohms unbalanced) or FMEC-DS1/E1 (for 120 ohms balanced)
    - Input impedance:  75 ohms unbalanced or 120 ohms balanced
    - Cable loss: 0 to 6 dB at 1024 kHz (for cable length, see the specification of the cable that you are using)
    - AIS: ITU-T G.704 compliant
- E1-N-14 Output
    - Bit rate: 2.048 MBit/s (Mbps) +/– 50 ppm
    - Frame format: Unframed, ITU-T G.704 framed
    - Line code: HDB-3
    - Termination: Via FMEC-E1 (for 75 ohms unbalanced) or FMEC-DS1/E1 (for 120 ohms balanced)
    - Output impedance:  75 ohms unbalanced or 120 ohms balanced
    - AIS: ITU-T G.704 compliant
    - Pulse shape: ITU-T G.703, Figure 15
    - Pulse amplitude: 2.37V +/– 5% zero-peak at 75 ohms; 3V +/– 5% zero-peak at 120 ohms

- Loopback modes: Terminal and Facility
- Environmental
  - Overvoltage protection: As in ITU-T G.703 Annex B
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 12.60W, 0.26A at –48V, 43.0 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.8 kg (1.9 lb)
- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.10  E3-12 Card

The twelve-port ONS 15454 SDH E3-12 card provides twelve ITU-compliant, G.703 E-3 ports per card. Each interface operates at 34.368 MBit/s (Mbps) over a 75-ohm coaxial cable (with FMEC-E3/DS3). The E3-12 card operates as a working or protect card in 1:1 protection schemes and as a working card in 1:N protection schemes. Figure 3-13 shows the E3-12 faceplates, and Figure 3-14 shows a block diagram of the card.

**Figure 3-13   E3-12 faceplate**
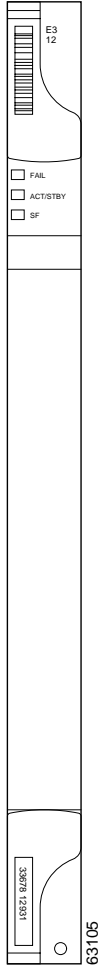


**Figure 3-14   E3-12 block diagram**
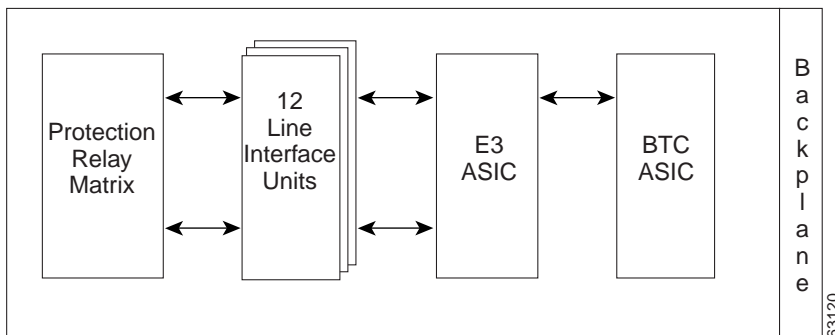


You can install the E3-12 card in any multispeed or high-speed card slot on the ONS 15454 SDH. Each E3-12 port features ITU-T G.703 compliant outputs supporting cable losses of up to 12 dB at 17184 kHz. The E3-12 card supports 1:1 protection.

**Note**  The lowest level cross-connect is STM-1. Lower level signals, such as E-1, DS-3, or E-3, can be dropped. This might leave part of the bandwidth unused.

**Note**  When a protection switch moves traffic from the E3-12 working/active card to the E3-12 protect/standby card, ports on the now active/standby card cannot be taken out of service. Lost traffic can result if you take a port out of service, even if the E3-12 active/standby card no longer carries traffic.

## 3.10.1  E3-12 Card-Level Indicators

The E3-12 card faceplate has three LEDs, described in Table 3-14.

*Table 3-14    E3-12 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the FAIL LED persists. |
| ACT/STBY LED<br>Green (Active)<br>Yellow (Standby) | When the ACTV/STBY LED is green, the E3-12 card is operational and ready to carry traffic. When the ACTV/STBY LED is yellow, the E3-12 card is operational and in standby (protect) mode. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as port LOS. |

## 3.10.2  E3-12 Port-Level Indicators

You can find the status of the twelve E3-12 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.10.3  E3-12 Specifications

- E3-12 Input
    - Bit rate: 34.368 MBit/s (Mbps) +/– 20 ppm
    - Line code: HDB-3
    - Termination: Unbalanced coaxial cable
    - Input impedance: 75 ohms +/–5%
    - Cable loss: Up to 12 dB at 17184 kHz (for cable length, see the specification of the cable that you are using)
    - AIS: ITU-T G.704 compliant
- E3-12 Output

- Bit rate: 34.368 MBit/s (Mbps) +/− 20 ppm

- Line code: HDB-3

- Termination: Unbalanced coaxial cable

- Output impedance: 75 ohms +/−5%

- AIS: ITU-T G.704 compliant

- Power level: −1.8 to +5.7 dBm

- Pulse shape: ITU-T G.703, Figure 17

- Pulse amplitude: 0.36 to 0.85V peak-to-peak

- Loopback modes: Terminal and Facility

- E3-12 Electrical Interface

  - Connectors: 1.0/2.3 Miniature Coax connectors in FMEC-E3/DS3

- Environmental

  - Overvoltage protection: As in ITU-T G.703 Annex B

  - Operating temperature: −5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

  - Operating humidity: 5 to 95%, noncondensing

  - Power consumption: 38.20W, 0.80A at −48V, 130.4 BTU/hr

- Dimensions

  - Height: 321.3 mm (12.650 in.)

  - Width: 18.2 mm (0.716 in.)

  - Depth: 228.6 mm (9.000 in.)

  - Depth with backplane connector: 235 mm (9.250 in.)

  - Weight not including clam shell: 0.7 kg (1.7 lb)

- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:

  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.11  DS3i-N-12 Card

The twelve-port ONS 15454 SDH DS3i-N-12 card provides twelve ITU-T G.703, Telcordia GR-499, and ITU-T G.704 compliant DS-3 ports per card. Each port operates at 44.736 MBit/s (Mbps) over a 75-ohm coaxial cable (with FMEC-E3/DS3).  The DS3i-N-12 can detect several different errored logic bits within a DS-3 frame. This function lets the ONS 15454 SDH identify a degrading DS-3 facility caused by upstream electronics (DS-3 Framer). In addition, DS-3 frame format auto detection and J1 path trace are supported. By monitoring additional overhead in the DS-3 frame, subtle network degradations can be detected. shows the DS3i-N-12 faceplate and shows a block diagram of the card.

*Figure 3-15   DS3i-N-12 faceplate*

DS3I- N
12

FAIL
ACT/STBY
SF

33678 12931

63110
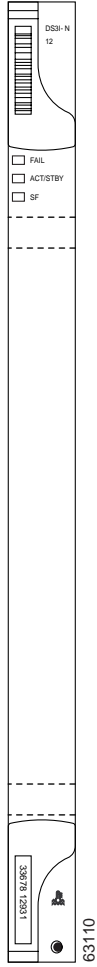
*Figure 3-16  DS3i-N-12 block diagram*
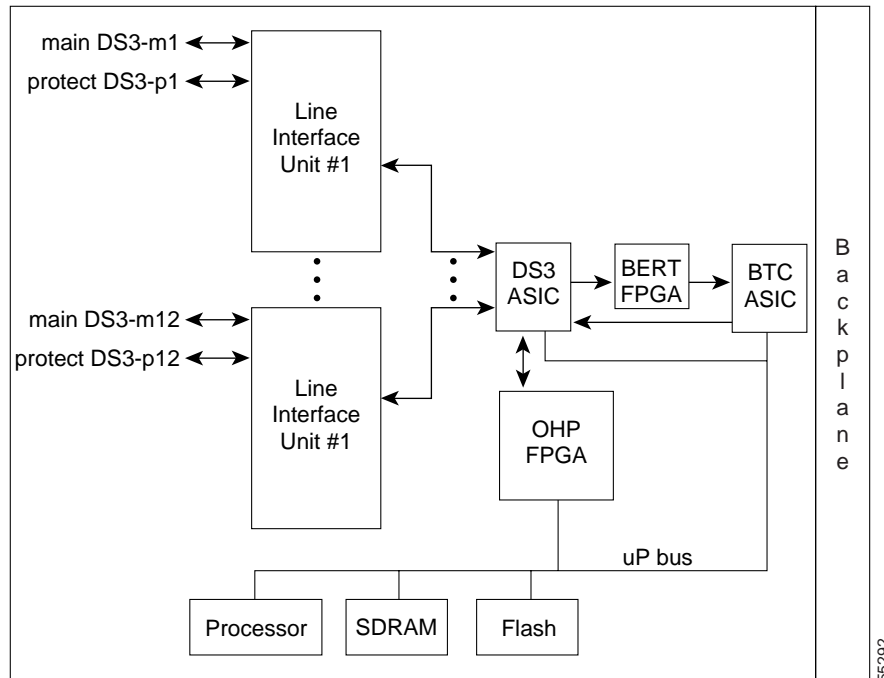


The following list summarizes the DS3i-N-12 card features:

- Provisionable framing format (M23, C-bit, or unframed)
- Auto-recognition and provisioning of incoming framing
- VC-3 payload mapping as per ITU-T G.707
- Idle signal ("1100") monitoring as per Telcordia GR-499
- P-bit monitoring
- C-bit parity monitoring
- X-bit monitoring
- M-bit monitoring
- F-bit monitoring
- Far-end block error (FEBE) monitoring
- Far-end alarm and control (FEAC) status and loop code detection
- Path trace byte support with TIM-P alarm generation

You can install the DS3i-N-12 card in any multispeed or high-speed card slot. Each DS3i-N-12 port features DSX-level outputs supporting distances up to 450 feet. With FMEC-E3/DS3, the card supports 1.0/2.3 Miniature Coax nonbalanced connectors.

The DS3i-N-12 can operate as the protect card in a 1:N (N ≤ 4) DS-3 protection group. It has circuitry that allows it to protect up to four working DS3i-N-12 cards.

**Note** The lowest level cross-connect is STM-1. Lower level signals, such as E-1, DS-3, or E-3, can be dropped. This might leave part of the bandwidth unused.

## 3.11.1 DS3i-N-12 Card-Level Indicators

The DS3i-N-12 card faceplate has three LEDs, listed in Table 3-15.

*Table 3-15    DS3i-N-12 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| ACT/STBY LED<br><br>Green (Active)<br><br>Yellow (Standby) | When the ACTV/STBY LED is green, the DS3i-N-12 card is operational and ready to carry traffic. When the ACTV/STBY LED is yellow, the DS3i-N-12 card is operational and in standby (protect) mode. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS or LOF on one or more of the card's ports. |

## 3.11.2 DS3i-N-12 Port-Level Indicators

You can find the status of the DS3i-N-12 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.11.3 DS3i-N-12 Card Specifications

- DS3i-N-12 Input
  - Bit rate: 44.736 MBit/s (Mbps) +/– 20 ppm
  - Frame format: ITU-T G.704, ITU-T G.752/DS-3 ANSI T1.107-1988
  - Line code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input impedance: 75 ohms +/–5%
  - Cable loss:
    Maximum 137 m (450 ft): 734A, RG59, 728A
    Maximum 24 m (79 ft): RG179
  - AIS: ITU-T G.704 compliant
- DS3i-N-12 Output
  - Bit rate: 44.736 MBit/s (Mbps) +/– 20 ppm
  - Frame format: ITU-T G.704 , ITU-T G.752/DS-3 ANSI T1.107-1988
  - Line code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Output impedance: 75 ohms +/–5%
  - AIS: ITU-T G.704 compliant

- Power level: –1.8 to +5.7 dBm (The power level is for a signal of all ones and is measured at a center frequency of 22.368 MHz (3 +/– 1 kHz) bandwidth.)
- Pulse shape: ITU-T G.703, Figure 14/ANSI T1.102-1988, Figure 8
- Pulse amplitude: 0.36 to 0.85V peak-to-peak
- Loopback modes: Terminal and Facility
- Line build out: 0 to 69 m (0 to 225 ft); 69 to 137 m (226 to 450 ft)
- DS3i-N-12 Electrical Interface
  - Connectors: 1.0/2.3 Miniature Coax connectors via FMEC-E3/DS3 card
- Environmental
  - Overvoltage protection: As in ITU-T G.703 Annex B
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 26.80W, 0.56A at –48V, 91.5 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.8 kg (1.9 lb)
- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

## 3.12  BLANK Card

The BLANK card provides EMC emission control for empty interface card slots. It also provides a way to close off the subrack front area, thus allowing air flow and convection to be maintained through the subrack. shows the BLANK card faceplate.

*Figure 3-17   BLANK faceplate*



33678 12031

61333
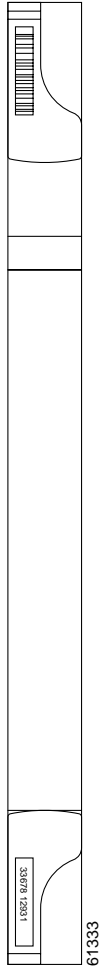
You have to install the BLANK in every empty interface card slot to maintain EMC requirements of the system and proper air flow.

# 3.12.1  BLANK Card Specifications

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: N/A
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Weight not including clam shell: 0.2 kg (0.4 lb)
- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:

– Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.13  FMEC-E1 Card

The ONS 15454 SDH FMEC-E1 card provides front mount electrical connection for fourteen ITU-compliant, G.703 E-1 ports. With FMEC-E1, each E1-N-14 port operates at 2.048 MBit/s (Mbps) over a 75-ohm unbalanced coaxial 1.0/2.3 Miniature Coax connector. Figure 3-18 shows the FMEC-E1 faceplate, and Figure 3-19 shows a block diagram of the card.

*Figure 3-18   FMEC-E1 faceplate*
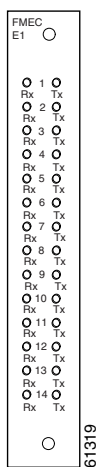


You can install the FMEC-E1 card in any EFCA (Electrical Facility Connection Assembly) slot from Slot 18 to 22 or Slot 25 to 29 on the ONS 15454 SDH. Each FMEC-E1 card port features E1-level inputs and outputs supporting cable losses of up to 6 dB at 1024 kHz.

*Figure 3-19   FMEC-E1 block diagram*
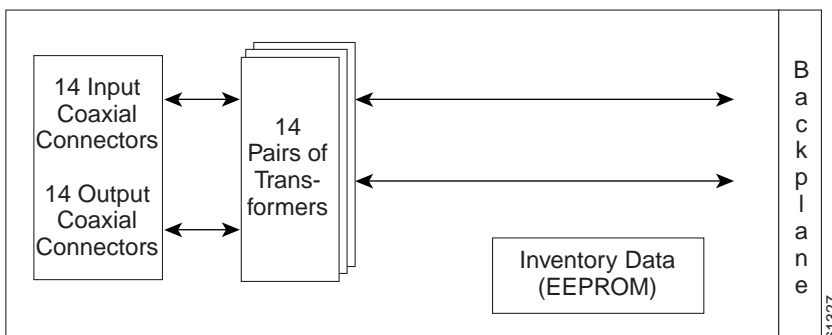
## 3.13.1 FMEC-E1 Specifications

- FMEC-E1 Input
    - Bit rate: 2.048 MBit/s (Mbps) + −50 ppm
    - Line code: HDB-3
    - Termination: Unbalanced coaxial cable
    - Input impedance: 75 ohms + −5%
    - Cable loss: Up to 6 dB at 1024 kHz
- FMEC-E1 Output
    - Bit rate: 2.048 MBit/s (Mbps) + −50 ppm
    - Line code: HDB-3
    - Termination: Unbalanced coaxial cable
    - Output impedance: 75 ohms + −5%
    - Pulse shape: ITU-T G.703, Figure 15 and Table 7
    - Pulse amplitude: ITU-T G.703, Figure 15 and Table 7
- FMEC-E1 Electrical Interface
    - Connectors: 1.0/2.3 Miniature Coax connectors
- Environmental
    - Operating temperature: −5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
    - Operating humidity: 5 to 95%, noncondensing
    - Power consumption: 0.00W, 0.00A at −48V, 0.0 BTU/hr
- Dimensions
    - Height: 182 mm (7.165 in.)
    - Width: 32 mm (1.25 in.)
    - Depth: 92 mm (3.62 in.)
    - Depth with backplane connector: 98 mm (3.87 in.)
    - Weight not including clam shell: 0.3 kg (0.7 lb)
- Compliance

    ONS 15454 SDH cards, when installed in a system, comply with these standards:
    - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

## 3.14  FMEC-E3/DS3 Card

The ONS 15454 SDH FMEC-E3/DS3 card provides front mount electrical connection for twelve ITU-compliant, G.703 E-3 or DS-3 ports. With FMEC-E3/DS3, each interface of an E3-12 card operates at 34.368 MBit/s (Mbps). Each interface of a DS3i-N-12 card operates at 44.736 MBit/s (Mbps) over a 75-ohm unbalanced coaxial 1.0/2.3 miniature coax connector. Figure 3-20 shows the FMEC-E3/DS3 faceplate and Figure 3-21 shows a block diagram of the card.

**Figure 3-20   FMEC-E3/DS3 faceplate**
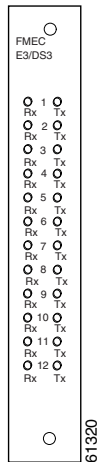


You can install the FMEC-E3/DS3 card in any EFCA slot from Slot 18 to 22 or Slot 25 to 29 on the ONS 15454 SDH. Each FMEC-E3/DS3 card interface features E3-level or DS3-level inputs and outputs supporting cable losses of up to 12 dB at 17184 kHz for E3 signals,  up to 137 m (450 ft) 734A, RG59, 728A per 24 m (79 ft) RG179 for DS3 signals.

**Figure 3-21   FMEC-E3/DS3 block diagram**
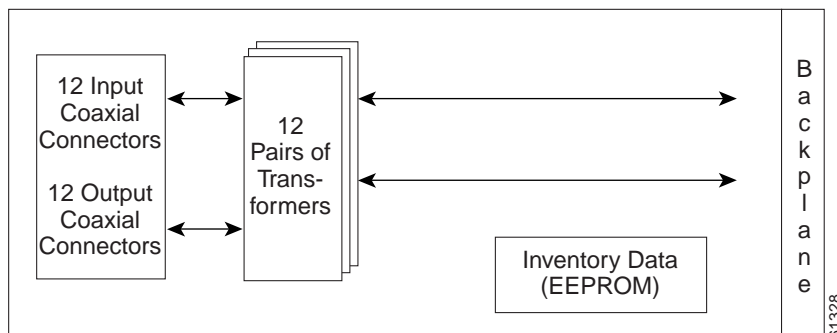


# 3.14.1  FMEC-E3/DS3 Card Specifications

- FMEC-E3/DS3 Input (for E3 signals)
    - Bit rate: 34.368 MBit/s (Mbps) +/– 20 ppm
    - Line code: HDB-3
    - Termination: Unbalanced coaxial cable
    - Input impedance: 75 ohms $+-5\%$
    - Cable loss: Up to 12 dB at 17184 kHz
- FMEC-E3/DS3 Output (for E3 signals)
    - Bit rate: 34.368 MBit/s (Mbps) +/– 20 ppm

Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4

- Line code: HDB-3

- Termination: Unbalanced coaxial cable

- Output impedance: 75 ohms +/−5%

- Pulse shape: ITU-T G.703, Figure 17

- Pulse amplitude: ITU-T G.703, Figure 17 and Table 9

- FMEC-E3/DS3 Input (for DS3 signals)

  - Bit rate: 44.736 MBit/s (Mbps) +/− 20 ppm

  - Line code: B3ZS

  - Termination: Unbalanced coaxial cable

  - Input impedance: 75 ohms +/−5%

  - Cable loss:
    Maximum 137 m (450 ft): 734A, RG59, 728A
    Max 24 m (79 ft): RG179

- FMEC-E3/DS3 Output (for DS3 signals)

  - Bit rate: 44.736 MBit/s (Mbps) +/− 20 ppm

  - Line code: B3ZS

  - Termination: Unbalanced coaxial cable

  - Output impedance: 75 ohms +/−5%

  - AIS: TR-TSY-000191 compliant

  - Power level: ITU-T G.703, Table 6; −1.8 to +5.7 dBm

  - Pulse shape: ITU-T G.703, Table 6 and Figure 14; ANSI T1.102-1988, Figure 8

  - Pulse amplitude: ITU-T G.703, Table 6; 0.36 to 0.85V peak-to-peak

  - Line build out: 0 to 225 ft; 226 to 450 ft

- FMEC-E3/DS3 Electrical Interface

  - Connectors: 1.0/2.3 Miniature Coax connectors

- Environmental

  - Operating temperature: −5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

  - Operating humidity: 5 to 95%, noncondensing

  - Power consumption: 0.00W, 0.00A at −48V, 0.0 BTU/hr

- Dimensions

  - Height: 182 mm (7.165 in.)

  - Width: 32 mm (1.25 in.)

  - Depth: 92 mm (3.62 in.)

  - Depth with backplane connector: 98 mm (3.87 in.)

  - Weight not including clam shell: 0.3 kg (0.7 lb)

- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:

  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

## 3.15  FMEC-DS1/E1 Card

The ONS 15454 SDH FMEC-DS1/E1 card provides front mount electrical connection for fourteen ITU-compliant, G.703 E-1 ports. With FMEC-DS1/E1, each E1-N-14 port operates at 2.048 MBit/s (Mbps) over a 120-ohm balanced cable via two 37-pin DB connectors.  Figure 3-22 shows the FMEC-DS1/E1 faceplate, and Figure 3-23 shows a block diagram of the card.

⚠

**Caution**    E1 ports on the DS1/E1 FMEC card can only be connected to Safety Extreme Low Voltage (SELV) circuits. The E1 interface is not intended for connection to any Australian Telecommunications network without the written consent of the network manager.

*Figure 3-22   FMEC-DS1/E1 faceplate*
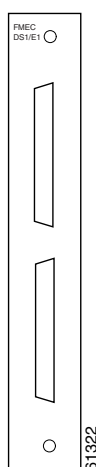


You can install the FMEC-DS1/E1 card in any EFCA slot from Slot 18 to 22 or Slot 25 to 29 on the ONS 15454 SDH. Each FMEC-DS1/E1 card interface features E1-level inputs and outputs supporting cable losses of up to 6 dB at 1024 kHz.

*Figure 3-23   FMEC-DS1/E1 block diagram*
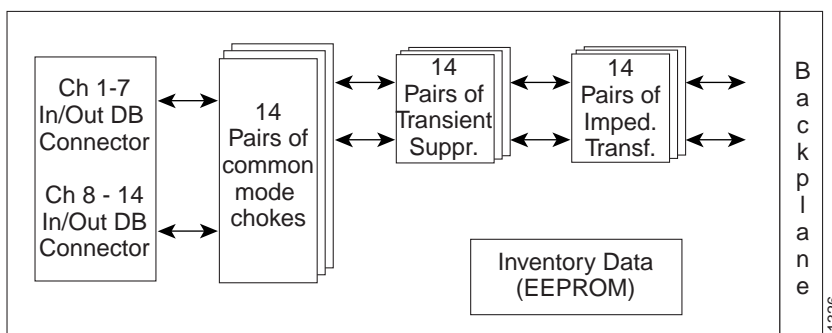
## 3.15.1 FMEC-DS1/E1 Card Specifications

- FMEC-DS1/E1 Input
  - Bit rate: 2.048 MBit/s (Mbps) +/−50 ppm
  - Line code: HDB-3
  - Termination: Balanced twisted pair cable
  - Input impedance: 120 ohms +/−5%
  - Cable loss: Up to 6 dB at 1024 kHz
- FMEC-DS1/E1 Output
  - Bit rate: 2.048 MBit/s (Mbps) +/−50 ppm
  - Line code: HDB-3
  - Termination: Balanced twisted pair cable
  - Output impedance: 120 ohms +/−5%
  - Pulse shape: ITU-T G.703, Figure 15 and Table 7
  - Pulse amplitude: ITU-T G.703, Figure 15 and Table 7
- FMEC-DS1/E1 Electrical Interface
  - Connectors: 37-pin DB connectors
- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 0.00W, 0.00A at –48V, 0.0 BTU/hr
- Dimensions
  - Height: 182 mm (7.165 in.)
  - Width: 32 mm (1.25 in.)
  - Depth: 92 mm (3.62 in.)
  - Depth with backplane connector: 98 mm (3.87 in.)
  - Weight not including clam shell: 0.3 kg (0.6 lb)
- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

## 3.16 FMEC-BLANK Card

The FMEC-BLANK card provides EMC emission control for empty FMEC slots. It also provides a way to close off the EFCA area, thus allowing air flow and convection to be maintained through the EFCA. Figure 3-24 shows the FMEC-BLANK card faceplate.

*Figure 3-24   FMEC-BLANK faceplate*
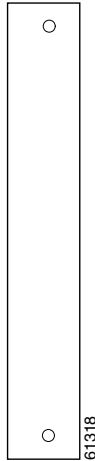


You have to install the BLANK FMEC in every empty FMEC slot to maintain EMC requirements of the system and proper air flow.

## 3.16.1  FMEC-BLANK Card Specifications

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: N/A
- Dimensions
  - Height: 182 mm (7.165 in.)
  - Width: 32 mm (1.25 in.)
  - Weight not including clam shell: 0.2 kg (0.4 lb)

# 3.17  MIC-A/P Card

The MIC-A/P card provides connection for one of the two possible redundant power supply inputs. It also provides connection for eight alarm outputs (coming from the TCC-I card) and for sixteen alarm inputs and four configurable alarm inputs/outputs. Its position is in Slot 23 in the center of the ONS 15454 SDH subrack EFCA area. Figure 3-25 on page 3-42 shows the MIC-A/P faceplate and Figure 3-26 on page 3-42 shows a block diagram of the card.

*Figure 3-25   MIC-A/P faceplate*
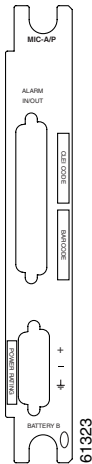


The following list summarizes MIC-A/P card features:

- Connection for one of the two possible redundant power supply inputs
- Connection for eight alarm outputs (coming from the TCC-I card)
- Connection for four configurable alarm inputs/outputs
- Connection for sixteen alarm inputs
- Storage of manufacturing and inventory data

**Note**    For proper system operation, both the MIC-A/P card and the MIC-C/T/P card must be installed in the shelf.

*Figure 3-26   MIC-A/P block diagram*
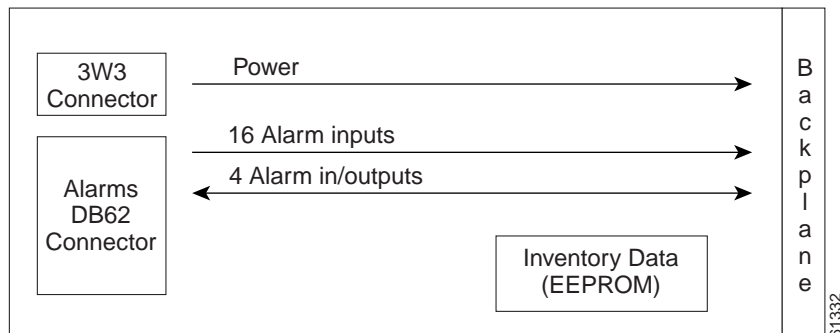


## 3.17.1 MIC-A/P Card Specifications

- MIC-A/P Power Supply Input
  - System supply voltage: Nominal –48 VDC
    Tolerance limits: –40.5 to –57.0 VDC

- Connector: 3WK3 Combo-D Power Cable Connector
- MIC-A/P Alarm Outputs
  - Voltage (open contact): Maximum 60 VDC
  - Current (closed contact): Maximum 250 mA
  - Connector: 62-pin DB connector (common for inputs/outputs)
- MIC-A/P Alarm Inputs
  - Voltage (open contact): Maximum 60 VDC
  - Current (closed contact): Maximum 2 mA
  - Connector: 62-pin DB connector (common for inputs/outputs)
- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 0.13W (provided by +5V from TCC-I), 0.44 BTU/hr
- Dimensions
  - Height: 182 mm (7.165 in.)
  - Width: 32 mm (1.25 in.)
  - Depth: 92 mm (3.62 in.)
  - Depth with backplane connector: 98 mm (3.87 in.)
  - Weight not including clam shell: 0.2 kg (0.5 lb)
- Compliance
  ONS 15454 SDH cards, when installed in a node, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.18  MIC-C/T/P Card

The MIC-C/T/P card provides connection for one of the two possible redundant power supply inputs. It also provides connection for system management serial port, system management LAN port, modem port (for future use), and system timing inputs and outputs. Place the MIC-C/T/P in Slot 24. shows the MIC-C/T/P card faceplate and shows a block diagram of the card.

*Figure 3-27   MIC-C/T/P faceplate*
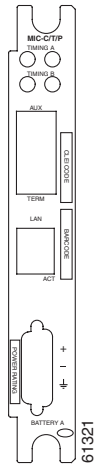


*Figure 3-28   MIC-C/T/P block diagram*
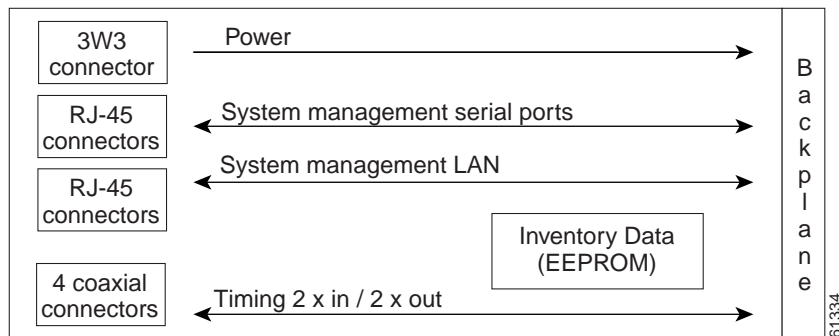


The following list summarizes MIC-C/T/P card features:

- Connection for one of the two possible redundant power supply inputs

- Connection for two serial ports for local craft/modem (for future use)

- Connection for one LAN port

- Connection for two system timing inputs

- Connection for two system timing outputs

- Storage of manufacturing and inventory data

**Note**    For proper system operation, both the MIC-A/P card and the MIC-C/T/P card must be installed in the shelf.

## 3.18.1 MIC-C/T/P Port-Level Indicators

The MIC-C/T/P card has one pair of LEDs, located on the RJ45 LAN connector. The green LED is illuminated when a link is present, and the yellow LED is illuminated when data is being transferred.

## 3.18.2 MIC-C/T/P Card Specifications

- MIC-C/T/P Power Supply Connector
  - System supply voltage: Nominal –48 VDC
    Tolerance limits: –40.5 to –57.0 VDC
  - Connector: 3WK3 Combo-D Power Cable Connector
- MIC-C/T/P Timing Connector
  - Frequency: 2.048 MHz $\neq$ −10 ppm
  - Signal level: 0.75 to 1.5V
  - Impedance: 75 ohms +/− 5% (switchable by jumper to high impedance > 3 kohms)
    (120 ohms impedance, balanced, possible with external matching cable)
  - Cable attenuation: Up to 6 dB at 2 MHz
  - Connectors: 1.0/2.3 Miniature Coax connector
- MIC-C/T/P Timing Connector
  - Frequency: 2.048 MHz $\neq$ −10 ppm
  - Signal level: 0.75 to 1.5V
  - Impedance: 75 ohms +/− 5%
    (120 ohms Impedance, balanced, possible with external matching cable)
  - Pulse mask: ITU-T G.703, Figure 20
  - Connectors: 1.0/2.3 Miniature Coax
- MIC-C/T/P System Management Serial Port:
  - System management serial port craft interface
  - Modem port (for future use)
  - Connectors: 8-pin RJ-45
- MIC-C/T/P System Management LAN Port Connectors:
  - Signal: 802.3 10 Base-T
  - Connectors: 8-pin RJ-45
- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 0.4W (provided by +5V from TCC-I), 1.37 BTU/hr
- Dimensions
  - Height: 182 mm (7.165 in.)
  - Width: 32 mm (1.25 in.)

        –  Depth: 92 mm (3.62 in.)

        –  Depth with backplane connector: 98 mm (3.87 in.)

        –  Weight not including clam shell: 0.2 kg (0.5 lb)

    •  Compliance

       ONS 15454 SDH cards, when installed in a system, comply with these standards:

        –  Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

# 3.19  OC3 IR 4/STM1 SH 1310 Card

The OC3 IR 4/STM1 SH 1310 card provides four intermediate or short range, ITU-T G.707- and G.957-compliant, SDH, STM-1 ports. Each port operates at 155.52 MBit/s (Mbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads at the STM-1 signal level on a per VC-4 basis. shows the OC3 IR 4/STM1 SH 1310 faceplate and shows a block diagram of the card.

⚠

**Warning**    **Class 1 laser product.**

*Figure 3-29   OC3 IR 4/STM1 SH 1310 faceplate*
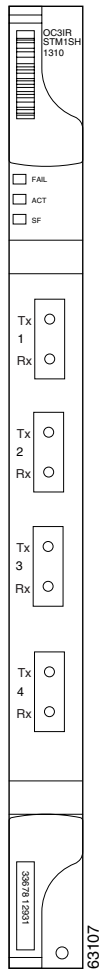
*Figure 3-30   OC3 IR 4/STM1 SH 1310 block diagram*
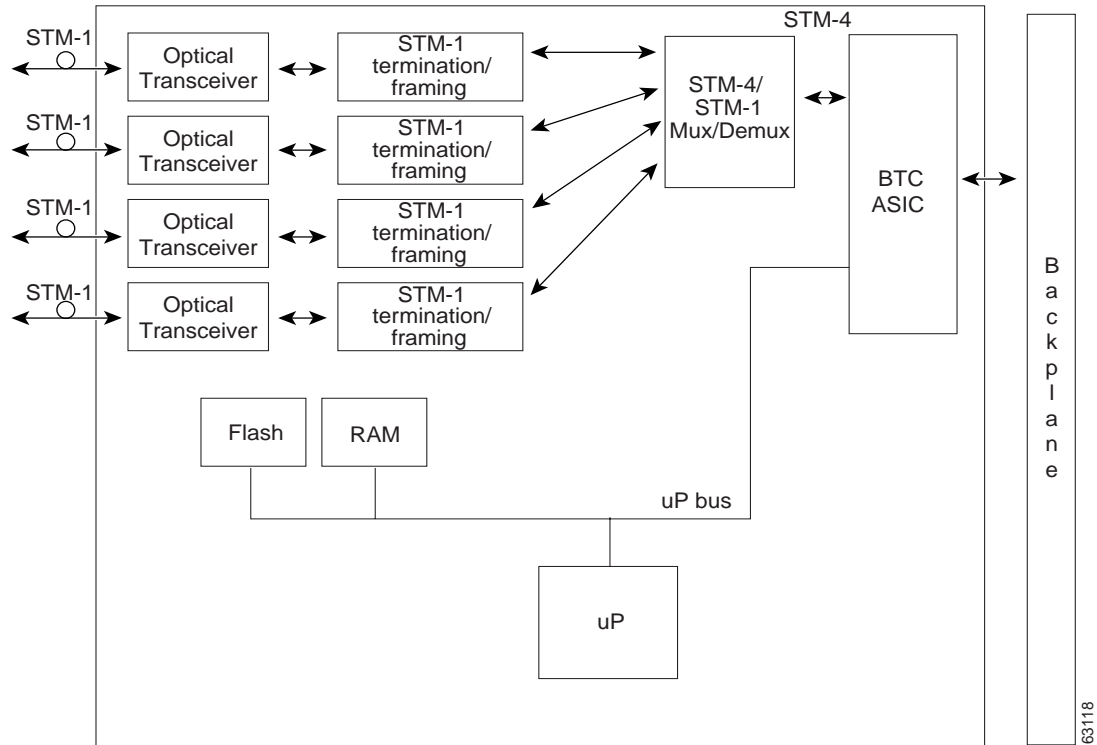


⚠

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

You can install the OC3 IR 4/STM1 SH 1310 card in any multispeed or high-speed card slot. The card can be provisioned as part of a SNCP or in an add/drop multiplexer/terminal monitor (ADM/TM) configuration. Each interface features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors.

The OC3 IR 4/STM1 SH 1310 card supports 1+1 unidirectional and bidirectional protection switching. You can provision protection on a per port basis.

The OC3 IR 4/STM1 SH 1310 detects LOS, LOF, loss of pointer (LOP), multiplex section alarm indication signal (MS-AIS), and multiplex section far-nd receive failure (MS-FERF) conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line bit interleaved parity (BIP) errors.

To enable automatic protection switching (APS), the OC3 IR 4/STM1 SH 1310 extracts the K1 and K2 bytes from the SDH overhead to perform appropriate protection switches. The DCC bytes are forwarded to the TCC-I, which terminates the DCC.

## 3.19.1  OC3 IR 4/STM1 SH 1310 Card-Level Indicators

The OC3 IR 4/STM1 SH 1310 card has three card-level LED indicators, described in Table 3-16.

*Table 3-16    OC3 IR 4/STM1 SH 1310 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| Green ACT LED | The green ACT LED indicates that the OC3 IR 4/STM1 SH 1310 card is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BER on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the links are working, the light turns off. |

### 3.19.1.1  OC3 IR 4/STM1 SH 1310 Port-Level Indicators

You can find the status of the four card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.19.2  OC3 IR 4/STM1 SH 1310 Card Specifications

- Line
  - Bit rate:155.52 MBit/s (Mbps)
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connector: SC
  - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1293 nm to 1334 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10
  - Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10
  - Receiver: InGaAs/InP photodetector
  - Link loss budget: 13 dB
  - Receiver Input Wavelength Range: 1274 nm – 1356 nm

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 19.20W, 0.40A at –48V, 65.6 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.4 kg (1.0 lb)
- Compliance
  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
  - Class 1 laser product

# 3.20  OC12 IR/STM4 SH 1310 Card

The OC12 IR/STM4 SH 1310 card provides one intermediate or short range, ITU-T G.707- and G.957-compliant, SDH STM-4 port per card. The interface operates at 622.08 MBit/s (Mbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads on a per VC-4 basis. Figure 3-31 on page 3-51 shows the OC12 IR/STM4 SH 1310 faceplate and Figure 3-32 on page 3-52 shows a block diagram of the card.

**Warning** **Class 1 laser product.**

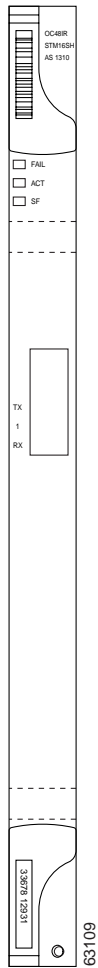**Figure 3-31   OC12 IR/STM4 SH 1310 faceplate**
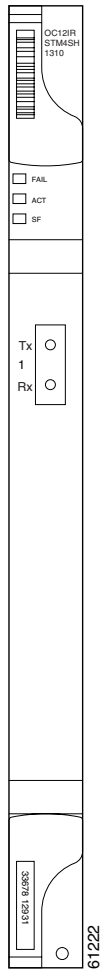
*Figure 3-32   OC12 IR/STM4 SH 1310 block diagram*
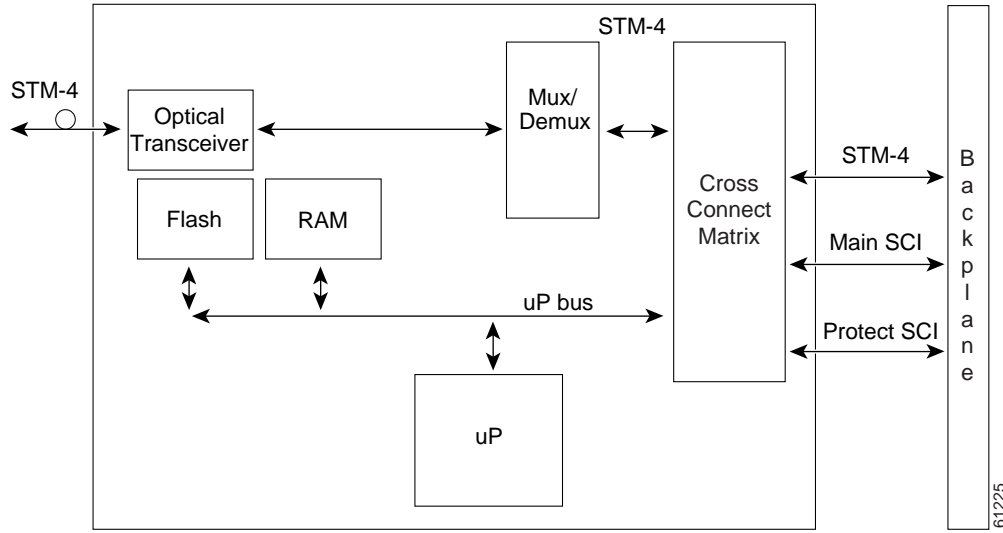


⚠

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

You can install the OC12 IR/STM4 SH 1310 card in any multispeed or high-speed card slot. You can provision the card as part of a multiplex section protection (MSP) or subnetwork connection (SNC) ring. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

The OC12 IR/STM4 SH 1310 card interface features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 IR/STM4 SH 1310 card uses SC optical connections and supports 1+1 unidirectional and bidirectional protection.

The OC12 IR/STM4 SH 1310 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card counts section and line BIP errors.

To enable MSP, the OC12 IR/STM4 SH 1310 extracts the K1 and K2 bytes from the SDH overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC-I card, which terminates the DCC.

## 3.20.1  OC12 IR/STM4 SH 1310 Card-Level Indicators

The OC12 IR/STM4 SH 1310 card has three card-level LED indicators, listed in Table 3-17.

*Table 3-17    OC12 IR/STM4 SH 1310 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| Green ACT LED | The green ACT LED indicates that the OC12 IR/STM4 SH 1310 card is operational and is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.20.2  OC12 IR/STM4 SH 1310 Port-Level Indicators

You can find the status of the OC12 IR/STM4 SH 1310 card port using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.20.3  OC12 IR/STM4 SH 1310 Card Specifications

- Line
  - Bit rate: 622.08 MBit/s (Mbps)
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1274 nm to 1356 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10
  - Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10
  - Receiver: InGaAs/InP photodetector
  - Link loss budget: 13 dB

- Receiver Input Wavelength Range: 1274 nm – 1356 nm
- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 10.90W, 0.23A at –48V, 37.2 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.6 kg (1.4 lb)
- Compliance
  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
  - Class 1 laser product

## 3.21  OC12 LR/STM4 LH 1310 Card

The OC12 LR/STM4 LH 1310 card provides one long-range, ITU-T G.707- and G.957-compliant, SDH STM-4 port per card. The interface operates at 622.08 MBit/s (Mbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads on a per VC-4 basis. Figure 3-33 on page 3-55 shows the OC12 LR/STM4 LH 1310 faceplate and Figure 3-34 on page 3-56 shows a block diagram of the card.

**Warning**    **Class 1 laser product.**
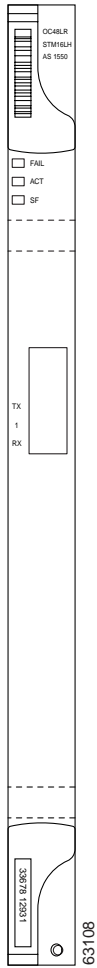
*Figure 3-33   OC12 LR/STM4 LH 1310 faceplate*
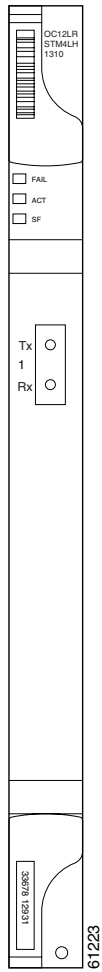
*Figure 3-34   OC12 LR/STM4 LH 1310 block diagram*
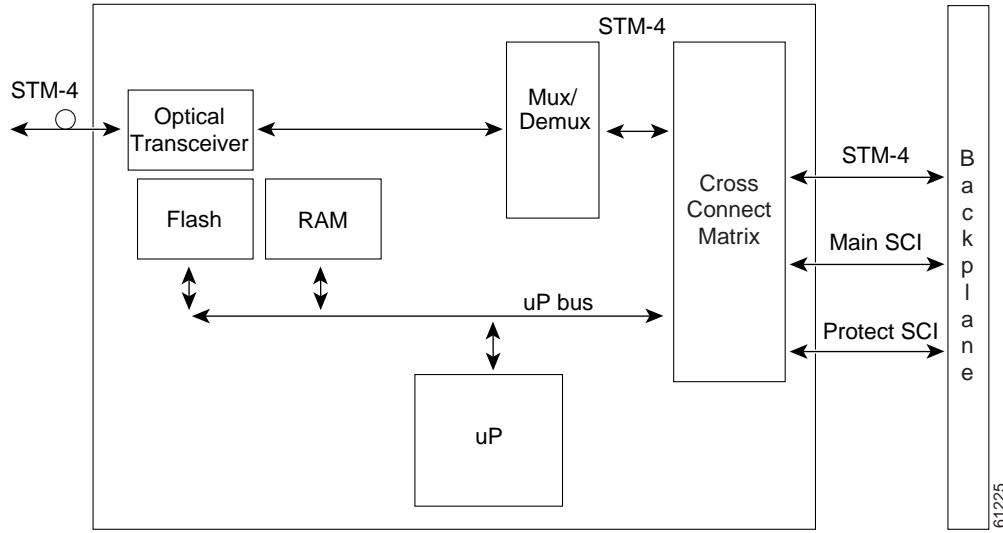


⚠

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

You can install the OC12 LR/STM4 LH 1310 card in any multispeed or high-speed card slot. You can provision the card as part of an MSP or SNC ring. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

The OC12 LR/STM4 LH 1310 card interface features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 LR/STM4 LH 1310 card uses SC optical connections and supports 1+1 unidirectional and bidirectional protection.

The OC12 LR/STM4 LH 1310 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line BIP errors.

To enable MSP, the OC12 LR/STM4 LH 1310 extracts the K1 and K2 bytes from the SDH overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC-I card, which terminates the DCC.

## 3.21.1  OC12 LR/STM4 LH 1310 Card-Level Indicators

The OC12 LR/STM4 LH 1310 card has three card-level LED indicators, listed in Table 3-18.

*Table 3-18   OC12 LR/STM4 LH 1310 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |

*Table 3-18    OC12 LR/STM4 LH 1310 Card-Level Indicators (continued)*

| Card-Level LEDs | Description |
|---|---|
| Green ACT LED | The green ACT LED indicates that the OC12 LR/STM4 LH 1310 card is operational and is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.21.2  OC12 LR/STM4 LH 1310 Port-Level Indicators

You can find the status of the OC12 LR/STM4 LH 1310 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.21.3  OC12 LR/STM4 LH 1310 Card Specifications

- Line
    - Bit rate: 622.08 MBit/s (Mbps)
    - Code: Scrambled NRZ
    - Fiber: 1310 nm single-mode
    - Loopback modes: Terminal and Facility
    - Connectors: SC
    - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
    - Maximum transmitter output power: +2 dBm
    - Minimum transmitter output power: –3 dBm
    - Center wavelength: 1280 nm to 1335 nm
    - Nominal wavelength: 1310 nm
    - Transmitter: Distributed feedback (DFB) laser
- Receiver
    - Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10
    - Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10
    - Receiver: InGaAs/InP photodetector
    - Link loss budget: 25 dB
    - Receiver Input Wavelength Range: 1280 nm – 1335 nm
- Environmental
    - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

- – Operating humidity: 5 to 95%, noncondensing
- – Power consumption: 9.28W, 0.19A at –48V, 31.7 BTU/hr
- Dimensions
  - – Height: 321.3 mm (12.650 in.)
  - – Width: 18.2 mm (0.716 in.)
  - – Depth: 228.6 mm (9.000 in.)
  - – Depth with backplane connector: 235 mm (9.250 in.)
  - – Weight not including clam shell: 0.6 kg (1.4 lb)
- Compliance
  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:
  - – Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
  - – Class 1 laser product

# 3.22  OC12 LR/STM4 LH 1550 Card

The OC12 LR/STM4 LH 1550 card provides one long-range, ITU-T G.707- and G.957-compliant, SDH STM-4 port per card. The interface operates at 622.08 MBit/s (Mbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads on a per VC-4 basis. shows the OC12 LR/STM4 LH 1550 faceplate and shows a block diagram of the card.

**Warning**    **Class 1 laser product.**

*Figure 3-35   OC12 LR/STM4 LH 1550 faceplate*

OC12LR
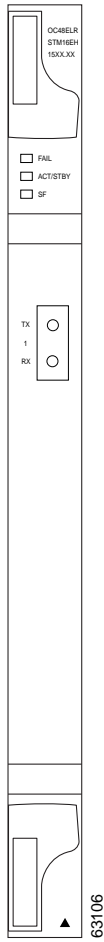STM4LH
1550

FAIL
ACT
SF

Tx
1
Rx

33678 12931

61224
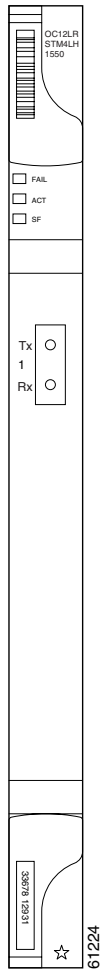
*Figure 3-36   OC12 LR/STM4 LH 1550 block diagram*
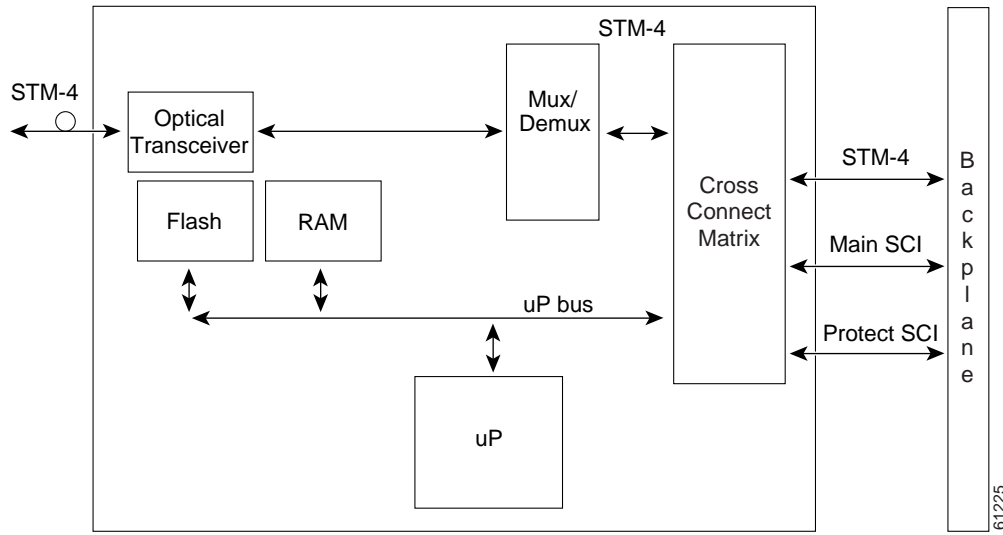


⚠️ **Warning**     **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

You can install the OC12 LR/STM4 LH 1550 card in any multispeed or high speed card slot. You can provision the card as part of an MSP or SNC ring. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

The OC12 LR/STM4 LH 1550 uses long-reach optics centered at 1550 nm and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 LR/STM4 LH 1550 uses SC optical connections and supports 1+1 bidirectional or unidirectional protection switching.

The OC12 LR/STM4 LH 1550 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line BIP errors.

To enable MSP, the OC12 LR/STM4 LH 1550 extracts the K1 and K2 bytes from the SDH overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC-I, which terminates the DCC.

## 3.22.1  OC12 LR/STM4 LH 1550 Card-Level Indicators

The OC12 LR/STM4 LH 1550 card has three card-level LED indicators, listed in Table 3-19.

*Table 3-19   OC12 LR/STM4 LH 1550 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |

*Table 3-19    OC12 LR/STM4 LH 1550 Card-Level Indicators (continued)*

| Card-Level LEDs | Description |
|---|---|
| Green ACT LED | The green ACT LED indicates that the OC12 LR/STM4 LH 1550 card is operational and ready to carry traffic. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.22.2  OC12 LR/STM4 LH 1550 Port-Level Indicators

You can find the status of the OC12 LR/STM4 LH 1550 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.22.3  OC12 LR/STM4 LH 1550 Card Specifications

- Line
  - Bit rate: 622.08 MBit/s (Mbps)
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: +2 dBm
  - Minimum transmitter output power: –3 dBm
  - Center wavelength: 1480 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: DFB laser
- Receiver
  - Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10
  - Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10
  - Receiver: InGaAs/InP photodetector
  - Link loss budget: 25 dB
  - Receiver Input Wavelength Range: 1480 nm – 1580 nm
- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

- – Operating humidity: 5 to 95%, noncondensing

- – Power consumption: 9.28W, 0.19A at –48V, 31.7 BTU/hr

- Dimensions

  - – Height: 321.3 mm (12.650 in.)

  - – Width: 18.2 mm (0.716 in.)

  - – Depth: 228.6 mm (9.000 in.)

  - – Depth with backplane connector: 235 mm (9.250 in.)

  - – Weight not including clam shell: 0.6 kg (1.4 lb)

- Compliance
  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

  - – Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11

  - – Class 1 laser product

# 3.23  OC12 IR/STM4 SH 1310-4 Card

The OC12 IR/STM4 SH 1310-4 card provides four intermediate or short range SDH STM-4 ports compliant with ITU-T G.707, and ITU-T G.957. Each port operates at 622.08 Mbps (MBits/s) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads on a per VC-4 basis. Figure 3-37 on page 3-63 shows the OC12 IR/STM4 SH 1310-4 faceplate and Figure 3-38 on page 3-64 shows a block diagram of the card.

**Warning**    **Class 1 laser product.**

*Figure 3-37   OC12 IR/STM4 SH 1310-4 faceplate*
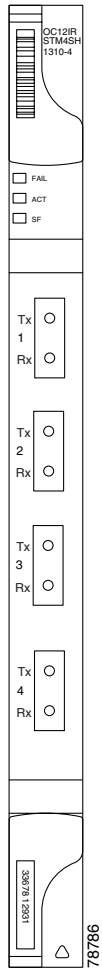
*Figure 3-38   OC12 IR/STM4 SH 1310-4 block diagram*
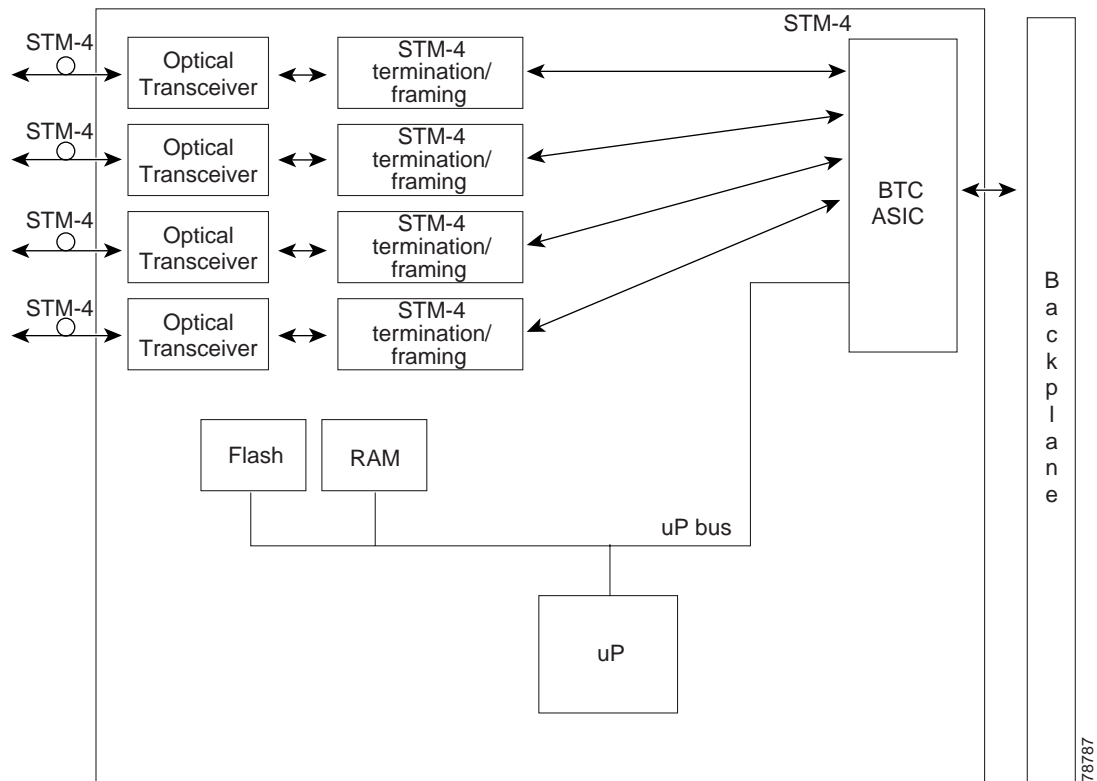


⚠

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

You can install the OC12 IR/STM4 SH 1310-4 card in any multispeed card slot (Slots 1 to 4 or 14 to 17). The card can be provisioned as part of an SNCP, of an MS-SPR, or in an ADM/TM configuration. Each interface features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors.

The OC12 IR/STM4 SH 1310-4 card supports 1+1 unidirectional and bidirectional protection switching. You can provision protection on a per port basis.

The OC12 IR/STM4 SH 1310-4 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4* for a description of these conditions. The card also counts section and line BIP errors.

Each port is configurable to support all ONS 15454 SDH configurations and can be provisioned as part of an MS-SPRing, SNCP, or MSP configuration.

To enable MSP, the OC12 IR/STM4 SH 1310-4 extracts the K1 and K2 bytes from the SDH overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC-I, which terminates the DCC.

**Note** If you ever expect to upgrade an OC-12/STM-4 ring to a higher bit rate, you should not put an OC12 IR/STM4 SH 1310-4 in that ring. The four-port card is not upgradable to a single-port card. The reason is that four different spans, possibly going to four different nodes, cannot be merged to a single span.

## 3.23.1  OC12 IR/STM4 SH 1310-4 Card-Level Indicators

The OC12 IR/STM4 SH 1310-4 card has three card-level LED indicators, listed in Table 3-20.

*Table 3-20    OC12 IR/STM4 SH 1310-4 Card-Level Indicators*

| Card-Level LEDs | Description |
| --- | --- |
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| Green ACT LED | The green ACT LED indicates that the OC12 IR/STM4 SH 1310-4 card is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BER on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the links are working, the light turns off. |

## 3.23.2  OC12 IR/STM4 SH 1310-4 Port-Level Indicators

You can find the status of the four card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide, R3.4* for a complete description of the alarm messages.

## 3.23.3  OC12 IR/STM4 SH 1310-4 Card Specifications

- Line
  - Bit rate: 622.08 Mbps (MBits/s)
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Chromatic Dispersion Allowance: 74 ps/nm for the spectral range of 1274 nm to 1356 nm; 46 ps/nm for the spectral range of 1293 nm to 1334 nm
  - Loopback modes: Terminal and Facility
  - Connector: SC
  - Compliance: Telcordia GR-253 IR-1, Telcordia GR-2918-CORE, ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: –8 dBm

- Minimum transmitter output power: –15 dBm

- Center wavelength: 1293 nm to 1334 nm

- Nominal wavelength: 1310 nm

- Transmitter: Fabry Perot laser

- Receiver

- Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10

- Minimum receiver level: –30 dBm at BER 1 * 10 exp – 10

- Receiver: InGaAs/InP photodetector

- Link loss budget: 15 dB

- Receiver Input Wavelength Range: 1274 nm to 1356 nm

- Environmental

- Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

- Operating humidity: 5 to 95%, noncondensing

- Power consumption: 28W, 0.58A at –48V, 95.6 BTU/hr

- Dimensions

- Height: 321.3 mm (12.650 in.)

- Width: 18.2 mm (0.716 in.)

- Depth: 228.6 mm (9.000 in.)

- Depth with backplane connector: 235 mm (9.250 in.)

- Weight not including clam shell: 0.4 kg (1.0 lb)

- Compliance

  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

- Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11

- Class 1 laser product

# 3.24  OC48 IR/STM16 SH AS 1310 Card

The OC48 IR/STM16 SH AS 1310 card provides one intermediate-range, ITU-T G.707- and G.957-compliant, SDH STM-16 port per card. The interface operates at 2.488 GBits/s (Gbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads at STM-1, STM-4, or STM-16 signal levels on a per VC-4 basis. Figure 3-39 shows the OC48 IR/STM16 SH AS 1310 faceplate and Figure 3-40 shows a block diagram of the card.

**Warning**    **Class 1 laser product.**

**Figure 3-39   OC48 IR/STM16 SH AS 1310 faceplate**

*Figure 3-40   OC48 IR/STM16 SH AS 1310 block diagram*
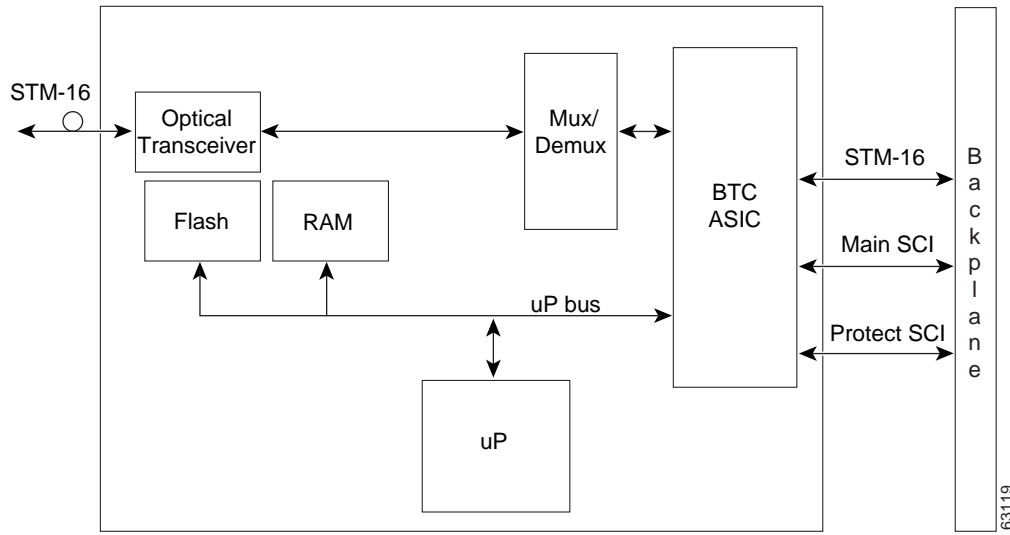


⚠ **Warning**    **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

You can install the OC48 IR/STM16 SH AS 1310 card in any multispeed or high-speed card slot on the ONS 15454 SDH. You can provision the card as part of a MS-SPRing or SNCP. In an ADM/TM configuration, you can provision the card as either an access tributary or a transport span interface.

The STM-16 port features a 1310-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC48 IR/STM16 SH AS 1310 uses SC connectors. The card supports 1+1 unidirectional protection and provisionable bidirectional switching.

The OC48 IR/STM16 SH AS 1310 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line BIP errors.

## 3.24.1  OC48 IR/STM16 SH AS 1310 Card-Level Indicators

The OC48 IR/STM16 SH AS 1310 card has three card-level LED indicators, listed in Table 3-21.

*Table 3-21   OC48 IR/STM16 SH AS 1310 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |

*Table 3-21    OC48 IR/STM16 SH AS 1310 Card-Level Indicators (continued)*

| Card-Level LEDs | Description |
|---|---|
| Green ACT LED | The green ACT LED indicates that the OC48 IR/STM16 SH AS 1310 card is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF, MS-AIS or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.24.2  OC48 IR/STM16 SH AS 1310 Port-Level Indicators

You can find the status of the OC48 IR/STM16 SH AS 1310 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.24.3  OC48 IR/STM16 SH AS 1310 Card Specifications

- Line
    - Bit rate: 2488.320 MBit/s (Mbps)
    - Code: Scrambled NRZ
    - Fiber: 1310 nm single-mode
    - Loopback modes: Terminal and Facility
    - Connectors: SC
    - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
    - Maximum transmitter output power: 0 dBm
    - Minimum transmitter output power: –5 dBm
    - Center wavelength: 1280 nm to 1350 nm
    - Nominal wavelength: 1310 nm
    - Transmitter: DFB laser
- Receiver
    - Maximum receiver level: 0 dBm at BER 1 * 10 exp – 10
    - Minimum receiver level: –18 dBm at BER 1 * 10 exp – 10
    - Receiver: InGaAs InP photodetector
    - Link loss budget: 13 dB minimum
    - Receiver Input Wavelength Range: 1280 nm – 1350 nm
- Environmental
    - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

- – Operating humidity: 5 to 95%, noncondensing
- – Power consumption: 37.20W, 0.78A at –48V, 127.0 BTU/hr
- Dimensions
  - – Height: 321.3 mm (12.650 in.)
  - – Width: 18.2 mm (0.716 in.)
  - – Depth: 228.6 mm (9.000 in.)
  - – Depth with backplane connector: 235 mm (9.250 in.)
  - – Weight not including clam shell: 0.9 kg (2.2 lb)
- Compliance

  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

  - – Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
  - – Class 1 laser product

# 3.25  OC48 LR/STM16 LH AS 1550 Card

The OC48 IR/STM16 SH AS 1310 card provides one long-range, ITU-T G.707- and G.957-compliant, SDH STM-16 port per card. The interface operates at 2.488 GBits/s (Gbps) over a single-mode fiber span. The card supports concatenated or non-concatenated payloads at STM-1, STM-4, or STM-16 signal levels on a per VC-4 basis. shows the OC48 LR/STM16 LH AS 1550 faceplate and shows a block diagram of the card.

**Warning**    **Class 1 laser product.**

**Figure 3-41    OC48 LR/STM16 LH AS 1550 faceplate**

OC48LR
STM16LH
AS 1550

FAIL
ACT
SF

TX
1
RX

33678 12931

63108

*Figure 3-42   OC48 LR/STM16 LH AS 1550 block diagram*
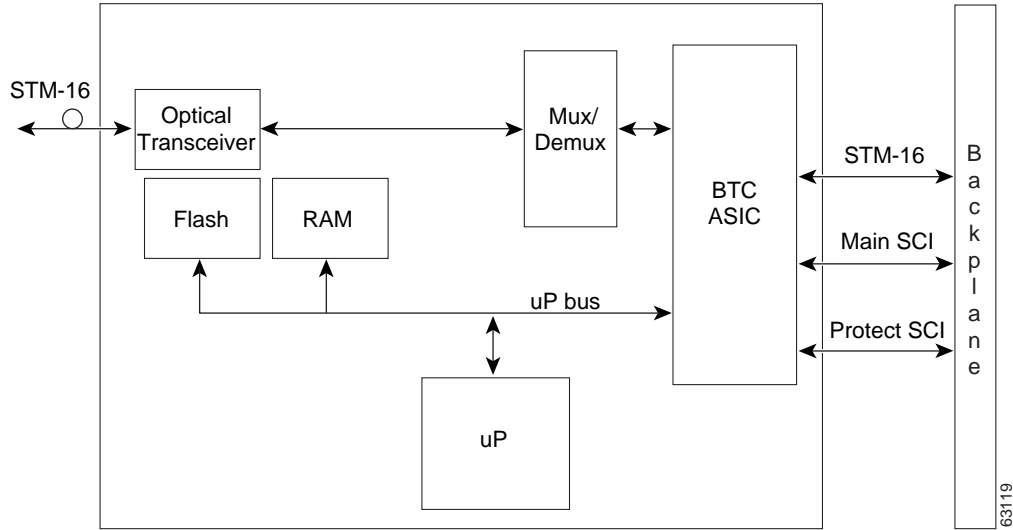


**Warning    Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

You can install OC48 LR/STM16 LH AS 1550 cards in any multispeed or high-speed slot on the ONS 15454 SDH. You can provision this card as part of a MS-SPRing or SNCP. In an ADM/TM configuration, you can provision the card as either an access tributary or a transport span interface.

The OC48 LR/STM16 LH AS 1550 port features a 1550 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors, and it supports 1+1 unidirectional protection and provisionable bidirectional and unidirectional switching.

The OC48 LR/STM16 LH AS 1550 detects LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line BIP errors.

## 3.25.1  OC48 LR/STM16 LH AS 1550 Card-Level Indicators

The OC48 LR/STM16 LH AS 1550 card has three card-level LED indicators, listed in Table 3-22.

*Table 3-22   OC48 LR/STM16 LH AS 1550 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |

*Table 3-22    OC48 LR/STM16 LH AS 1550 Card-Level Indicators (continued)*

| Card-Level LEDs | Description |
|---|---|
| Green ACT LED | The green ACT LED indicates that the OC48 LR/STM16 LH AS 1550 card is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.25.2  OC48 LR/STM16 LH AS 1550 Port-Level Indicators

You can find the status of the OC48 LR/STM16 LH AS 1550 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.25.3  OC48 LR/STM16 LH AS 1550 Card Specifications

- Line
  - Bit rate: 2488.320 MBit/s (Mbps)
  - Code: Scrambled NRZ
  - Fiber: 1550 nm Single Mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: +3 dBm
  - Minimum transmitter output power: –2 dBm
  - Center wavelength: 1520 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: DFB laser
- Receiver
  - Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10
  - Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10
  - Receiver: InGaAs APD photodetector
  - Link loss budget: 26 dB minimum, with 1 dB dispersion penalty
  - Receiver Input Wavelength Range: 1520 nm – 1580 nm
- Environmental
  - Eye safety compliance: Class 1 (EN60825)

> – Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
>
> – Operating humidity: 5 to 95%, noncondensing
>
> – Power consumption: 37.20W, 0.78A at –48V, 127.0 BTU/hr

- Dimensions

> – Height: 321.3 mm (12.650 in.)
>
> – Width: 18.2 mm (0.716 in.)
>
> – Depth: 228.6 mm (9.000 in.)
>
> – Depth with backplane connector: 235 mm (9.250 in.)
>
> – Weight not including clam shell: 0.9 kg (2.2 lb)

- Compliance

ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

> – Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
>
> – Class 1 laser product

# 3.26  OC48 ELR/STM16 EH 100 GHz Cards

Eighteen distinct STM-16 ITU 100 GHz DWDM cards comprise the ONS 15454 SDH DWDM channel plan. This plan contains every second in a series of 100-GHz-spaced wavelengths. Though the ONS 15454 SDH only uses 200-GHz spacing, the cards work in 100-GHz-spaced nodes, as well. Each OC48 ELR/STM16 EH 100 GHz card provides one SDH STM-16 port compliant with ITU-T G.692, ITU-T G.707, ITU-T G.957, and ITU-T G.958. The interface operates at 2.488 GBits/s (Gbps) over a single-mode fiber span. Each card supports concatenated or non-concatenated payloads at STM-1, STM-4, or STM-16 signal levels on a per VC-4 basis. Figure 3-43 on page 3-75 shows the OC48 ELR/STM16 EH 100 GHz faceplate and Figure 3-44 on page 3-76 shows a block diagram of the card.

**Warning**    **Class 1 laser product.**

**Figure 3-43   OC48 ELR/STM16 EH 100 GHz faceplate**
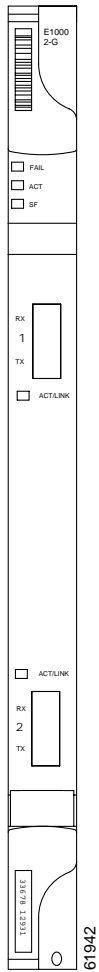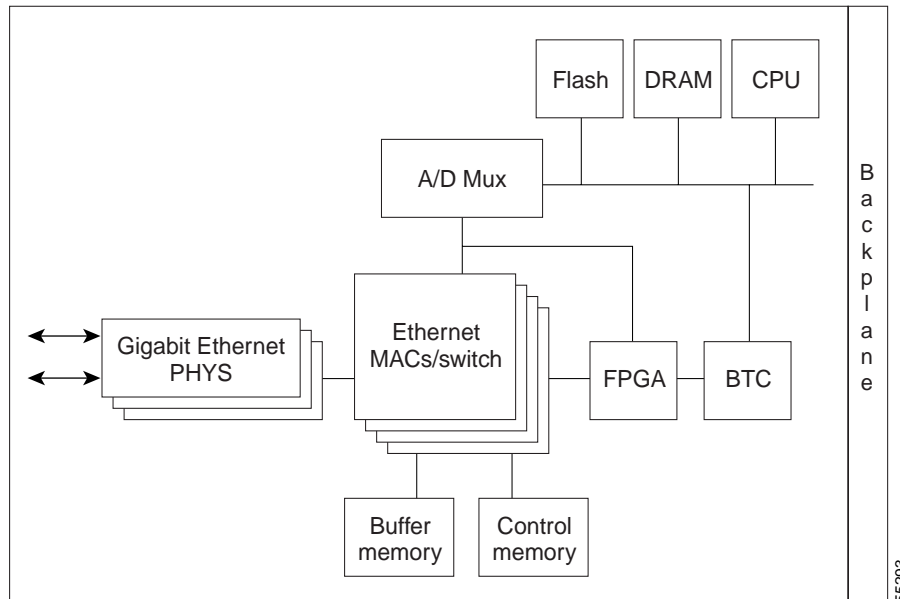
*Figure 3-44   STM-16SH-ELH 15XX.XX (DWDM) block diagram*
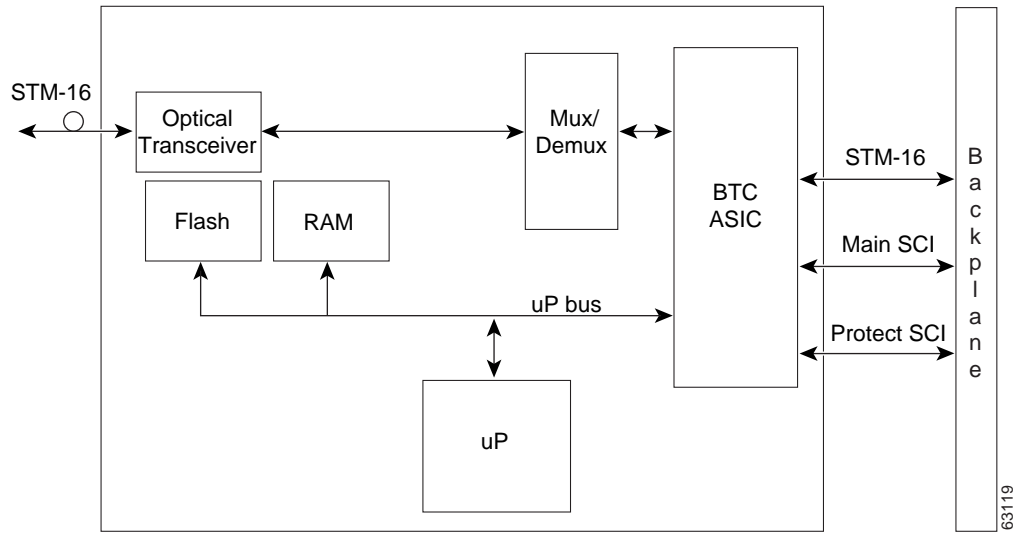


⚠

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

Nine of the cards operate in the blue band with a spacing of 2 * 100 GHz in the ITU grid (1530.33 nm, 1531.90 nm, 1533.47 nm, 1535.04 nm, 1536.61 nm, 1538.19 nm, 1539.77 nm, 1541.35 nm, and 1542.94 nm). The other nine cards operate in the red band with a spacing of 2 * 100 GHz in the ITU grid (1547.72 nm, 1549.32 nm, 1550.92 nm, 1552.52 nm, 1554.13 nm, 1555.75 nm, 1557.36 nm, 1558.98 nm, and 1560.61 nm).

You can install the OC48 ELR/STM16 EH 100 GHz cards in any high-speed slot. You can provision this card as part of a MS-SPRing or SNCP. In an ADM/TM configuration, you can provision the card as either an access tributary or a transport span interface.

✎

**Note**    Slots 5, 6, 12, and 13 are high-speed slots.

Each OC48 ELR/STM16 EH 100 GHz card uses extended long-reach optics operating individually within the ITU 100-GHz grid. The OC48 ELR/STM16 EH 100 GHz cards are intended to be used in applications with long unregenerated spans of up to 200 km (with mid-span amplification). These transmission distances are achieved through the use of inexpensive optical amplifiers (flat gain amplifiers) such as erbium-doped fiber amplifiers (EDFAs). Using co-located amplification, distances up to 200 km can be achieved for a single channel (160 km for 8 channels).

Maximum system reach in filterless applications is 24 dB or approximately 80 km without the use of optical amplifiers or regenerators. However, system reach also depends on the condition of the facilities, number of splices and connectors, and other performance-affecting factors. The OC48 ELR/STM16 EH 100 GHz cards feature wavelength stability of ≠ −0.25 nm. Each port contains a transmitter and a receiver.

The OC48 ELR/STM16 EH 100 GHz cards are the first in a family of cards meant to support extended long-reach applications in conjunction with optical amplification. Using DFB laser technology, the OC48 ELR/STM16 EH 100 GHz cards provide a solution at the lower extended long-reach distances.

The OC48 ELR/STM16 EH 100 GHz port features a 1550-nm range laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors and supports 1+1 unidirectional and bidirectional protection switching.

The OC48 ELR/STM16 EH 100 GHz cards detect LOS, LOF, LOP, MS-AIS, and MS-FERF conditions. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The cards also count section and line BIP errors.

To enable MSP, the OC48 ELR/STM16 EH 100 GHz cards extract the K1 and K2 bytes from the SDH overhead. The DCC bytes are forwarded to the TCC-I card; the TCC-I terminates the DCC.

## 3.26.1  OC48 ELR/STM16 EH 100 GHz Card-Level Indicators

The OC48 ELR/STM16 EH 100 GHz cards have three card-level LED indicators, listed in Table 3-23.

*Table 3-23    OC48 ELR Card-Level Indicators*

| Card-Level LEDs | Description |
| --- | --- |
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| Green ACT LED | The green ACT LED indicates that the OC48 ELR/STM16 EH 100 GHz card is carrying traffic or is traffic-ready. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.26.2  OC48 ELR/STM16 EH 100 GHz Port-Level Indicators

You can find the status of the OC48 ELR/STM16 EH 100 GHz card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.26.3  OC48 ELR/STM16 EH 100 GHz Card Specifications

- Line
    - Bit rate: 2488.320 MBit/s (Mbps)
    - Code: Scrambled NRZ
    - Fiber: 1550 nm single-mode
    - Loopback modes: Terminal and Facility
    - Connectors: SC
    - Compliance: ITU-T G.692, ITU-T G.707, ITU-T G.957, ITU-T G.958
- Transmitter

- – Maximum transmitter output power: 0 dBm

- – Minimum transmitter output power: –2 dBm

- – Center wavelength: ± 0.25 nm

- – Transmitter: DFB laser

- Receiver

    - – Maximum receiver level: –8 dBm at BER 1 * 10 exp – 10

    - – Minimum receiver level: –28 dBm at BER 1 * 10 exp – 10

    - – Receiver: InGaAs APD photodetector

    - – Link loss budget: 26 dB minimum, with 1 dB dispersion penalty

    - – Receiver Input Wavelength Range: 1520 nm – 1580 nm

- Environmental

    - – Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

    - – Operating humidity: 5 to 95%, noncondensing

    - – Power consumption: 31.20W, 0.65A at –48V, 106.5 BTU/hr

- Dimensions

    - – Height: 321.3 mm (12.650 in.)

    - – Width: 18.2 mm (0.716 in.)

    - – Depth: 228.6 mm (9.000 in.)

    - – Depth with backplane connector: 235 mm (9.250 in.)

    - – Weight not including clam shell: 1.1 kg (2.4 lb)

- Compliance

    ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

    - – Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11

    - – Class 1 laser product

- Currently available wavelengths and versions of OC48 ELR/STM16 EH 100 GHz:

    2 * 100 GHz spacing ITU grid blue band:

    - – 1530.33 +/−0.25 nm, STM-16HS-ELH 1530.33 (DWDM)

    - – 1531.90 +/−0.25 nm, STM-16HS-ELH 1531.90 (DWDM)

    - – 1533.47 +/−0.25 nm, STM-16HS-ELH 1533.47 (DWDM)

    - – 1535.04 +/−0.25 nm, STM-16HS-ELH 1535.04 (DWDM)

    - – 1536.61 +/−0.25 nm, STM-16HS-ELH 1536.61 (DWDM)

    - – 1538.19 +/−0.25 nm, STM-16HS-ELH 1538.19 (DWDM)

    - – 1539.77 +/−0.25 nm, STM-16HS-ELH 1539.77 (DWDM)

    - – 1541.35 +/−0.25 nm, STM-16HS-ELH 1541.35 (DWDM)

    - – 1542.94 +/−0.25 nm, STM-16HS-ELH 1542.94 (DWDM)

    2 * 100 GHz spacing ITU grid red band:

    - – 1547.72 +/−0.25 nm, STM-16HS-ELH 1547.72 (DWDM)

- 1549.32 +/–0.25 nm, STM-16HS-ELH 1549.32 (DWDM)

- 1550.92 +/–0.25 nm, STM-16HS-ELH 1550.92 (DWDM)

- 1552.52 +/–0.25 nm, STM-16HS-ELH 1552.52 (DWDM)

- 1554.13 +/–0.25 nm, STM-16HS-ELH 1554.13 (DWDM)

- 1555.75 +/–0.25 nm, STM-16HS-ELH 1555.75 (DWDM)

- 1557.36 +/–0.25 nm, STM-16HS-ELH 1557.36 (DWDM)

- 1558.98 +/–0.25 nm, STM-16HS-ELH 1558.98 (DWDM)

- 1560.61 +/–0.25 nm, STM-16HS-ELH 1560.61 (DWDM)

# 3.27  OC192 LR/STM64 LH 1550 Card

**Note**      Due to the high output power (+7 dBm to +10 dBm), a laser warning is printed on the faceplate of the OC192 LR/STM64 LH 1550 card. A safety key lock is added above the optical connectors to shut down the laser in order to prevent possible eye damage when the card is powered and the optical fibers are unconnected.

**Warning**      **Class 1 (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products. Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments, or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**      Use of controls or adjustments, or performance of procedures other than those specified might result in hazardous radiation exposure.

*Figure 3-45   OC192 LR/STM64 LH 1550 faceplate*
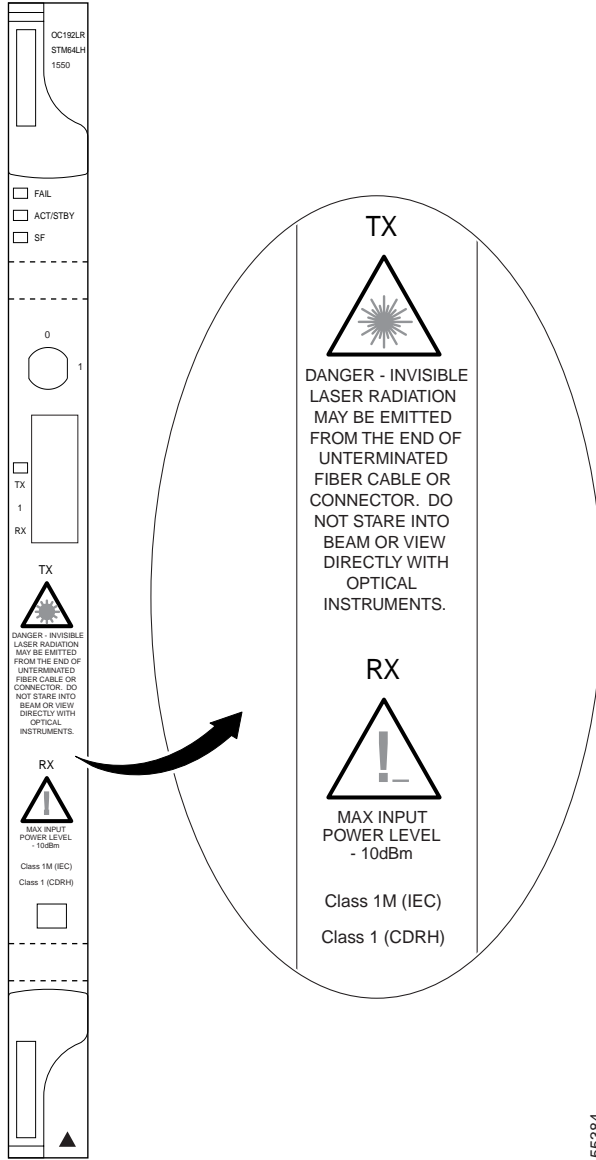
*Figure 3-46   OC192 LR/STM64 LH 1550 block diagram*

The OC192 LR/STM64 LH 1550 card provides one long-range, ITU-T G.707- and G.957-compliant, SDH STM-64 port per card. Also, the port is compliant to ITU-T G.691 (prepublished unedited version 10/2000) L-64.2, except for optical output power and receiver sensitivity (see the note in OC192 LR/STM64 LH 1550 Card Specifications, page 3-82). The port operates at 9.95328 GBits/s (Gbps) over unamplified distances up to 80 km with different types of fiber such as C-SMF or dispersion compensated fiber limited by loss and/or dispersion. The card supports concatenated or non-concatenated payloads on a VC-4 basis, as well as VC-4, VC-3, and VC-12 payloads. Figure 3-45 shows the OC192 LR/STM64 LH 1550 faceplate and Figure 3-46 shows a block diagram of the card.

**Note**    You must use a 20-dB fiber attenuator (19 to 24 dB) when working with the OC192 LR/STM64 LH 1550 card in a loopback. Do not use fiber loopbacks with the OC192 LR/STM64 LH 1550 card. Using fiber loopbacks causes irreparable damage to the OC192 LR/STM64 LH 1550 card.

You can install OC192 LR/STM64 LH 1550 cards in any high-speed slot on the ONS 15454 SDH. You can provision this card as part of an MS-SPRing, SNCP, or linear configuration or also as a regenerator for longer span reaches.

The OC192 LR/STM64 LH 1550 port features a 1550-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses a dual SC connector for optical cable termination. The card supports 1+1 unidirectional and bidirectional facility protection. It also supports 1:1 protection in four-fiber bidirectional line switched ring applications where both span switching and ring switching might occur.

The OC192 LR/STM64 LH 1550 card detects SF, LOS, or LOF conditions on the optical facility. Refer to Chapter 1, "Alarm Troubleshooting," for a description of these conditions. The card also counts section and line BIP errors from B1 and B2 byte registers in the section and line overhead.

## 3.27.1  OC192 LR/STM64 LH 1550 Card-Level Indicators

The OC192 LR/STM64 LH 1550 card has three card-level LED indicators, listed in Table 3-24.

*Table 3-24   OC192 LR/STM64 LH 1550 Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready. This LED is lit during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists. |
| ACT/STBY LED<br><br>Green (Active)<br><br>Yellow (Standby) | When the ACTV/STBY LED is green, the OC192 LR/STM64 LH 1550 card is operational and ready to carry traffic. When the ACTV/STBY LED is yellow, the OC192 LR/STM64 LH 1550 card is operational and in standby (protect) mode. |
| Yellow SF LED | The yellow SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on one or more of the card's ports. The yellow SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected and the link is working, the light turns off. |

## 3.27.2  OC192 LR/STM64 LH 1550 Port-Level Indicators

You can find the status of the OC192 LR/STM64 LH 1550 card ports using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

## 3.27.3  OC192 LR/STM64 LH 1550 Card Specifications

- Line
  - Bit rate: 9.95328 GBits/s (Gbps)
  - Code: Scrambled NRZ
  - Fiber: 1550 nm Single Mode
  - Maximum chromatic dispersion allowance: 1600 ps/nm

⚠
**Caution**     You must use a 20 dB fiber attenuator (19 to 24dB) when working with the OC192 LR/STM64 LH 1550 card in a loopback. Do not use fiber loopbacks with these cards.

  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: ITU-T G.707, ITU-T G.957
- Transmitter
  - Maximum transmitter output power: +10 dBm (see Note on page 3- 83)
  - Minimum transmitter output power: +7 dBm (see Note on page 3- 83)
  - Center wavelength: 1545 nm to 1555 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: LN (Lithium Niobate) external modulator transmitter

- Receiver

  - Maximum receiver level: –9 dBm at BER 1 * 10 exp – 12 (see Note on page 3- 83)

  - Minimum receiver level: –17 dBm at BER 1 * 10 exp – 12 (see Note on page 3- 83)

  - Receiver: APD/TIA

  - Link loss budget: 24 dB minimum, with no dispersion or 22 dB optical path loss at BER = 1 * 10 exp – 12 including dispersion

  - Receiver Input Wavelength Range: 1545 nm – 1555 nm

- Environmental

  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)

  - Operating humidity: 5 to 95%, noncondensing

  - Power consumption: 72.20W, 1.50A at –48V, 246.5 BTU/hr

- Dimensions

  - Height: 321.3 mm (12.650 in.)

  - Width: 18.2 mm (0.716 in.)

  - Depth: 228.6 mm (9.000 in.)

  - Depth with backplane connector: 235 mm (9.250 in.)

  - Weight not including clam shell: 1.3 kg (3.1 lb)

- Compliance

  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11

  - Class 1M (IEC 60825-1 2001.01) and class I (21 CFR 1040.10 and 1040.11) laser product

**Note**    The optical output power of the OC192 LR/STM64 LH 1550 (+7 dBm to +10 dBm) is 3 dB lower than in L-64.2b of the pre-published unedited version 10/2000 of ITU-T G.691 (+10 dBm to +13 dBm). However, the total attenuation range of the optical path, 22 to 16 dB, is maintained by the optical receiver sensitivity range of the OC192 LR/STM64 LH 1550 (–9 dBm to –17 dBm). This sensitivity range outperforms the specification in L-64.2b of the pre-published unedited version 10/2000 of ITU-T G.691 (–14 dBm to –3 dBm).

## 3.28  E100T-G Card

The E100T-G card provides twelve ports of IEEE 802.3-compliant, 10/100 interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 MBit/s (Mbps) per port and 2.488 GBits/s (Gbps) per card. Each port independently detects the speed of an attached device (auto-senses) and automatically connects at the appropriate speed. The ports auto-configure to operate at either half or full duplex and can determine whether to enable or disable flow control. Figure 3-47 on page 3-84 shows the card faceplate and Figure 3-48 on page 3-85 shows a block diagram of the card.

*Figure 3-47   E100T-G faceplate*
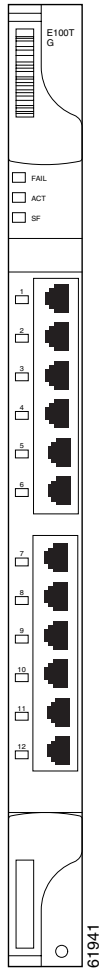
**Figure 3-48   E100T-G block diagram**
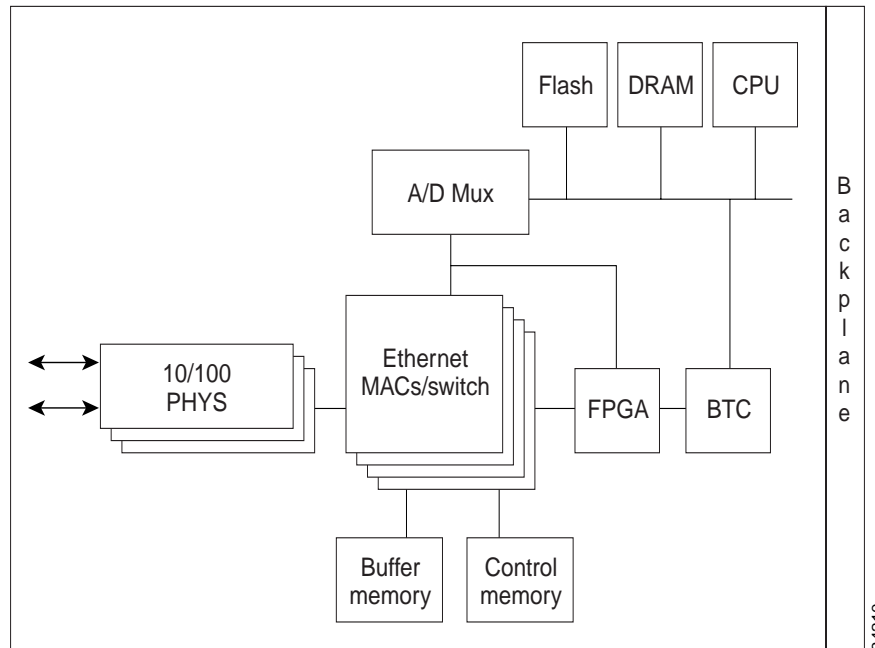


The E100T-G Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across an SDH/SONET network while providing a greater degree of reliability through SDH/SONET "self-healing" protection services. This Ethernet capability enables network operators to provide multiple 10/100 MBit/s (Mbps) access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic are provided.

The E100T-G eliminates the need for external aggregation equipment such as Ethernet switches, remote headends or distributed points of presence (POPs).

Each E100T-G card supports standards-based, wire-speed, Layer 2 Ethernet switching between its Ethernet ports. The 802.1Q tag and port-based VLANs logically isolate traffic (typically subscribers). Priority queuing is also supported to provide multiple classes of service.

You can install the E100T-G card in any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 SDH act as a single switch supporting a variety of SDH/SONET port configurations. You can create logical SDH/SONET ports by provisioning a number of VC-4 channels to the packet switch entity within the ADM. Logical ports can be created with a bandwidth granularity of VC-4. The ONS 15454 SDH supports VC-4-1c, VC-4-2c, or VC-4-4c signal levels.

## 3.28.1  E100T-G Card-Level Indicators

The E100T-G card faceplate has two card-level LED indicators, listed in .

*Table 3-25   E100T-G Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready or catastrophic software failure occurred on the E100T-G card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational. |
| Green ACT LED | A green ACT LED provides the operational status of the E100T-G. When the ACT LED is green it indicates that the E100T-G card is active and the software is operational. |
| SF LED | Not used |

## 3.28.2  E100T-G Port-Level Indicators

The E100T-G card also has twelve pairs of LEDs (one pair for each port) to indicate port conditions. A green L LED indicates that a link is detected. A yellow A LED indicates an active connection. If the A LED is off it indicates an inactive connection or unidirectional traffic. The port-level indicators are described in Table 3-26.

You can find the status of the E100T-G card port using the LCD screen on the ONS 15454 SDH fan-tray assembly. Use the LCD to view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. Refer to Chapter 1, "Alarm Troubleshooting," for a complete description of the alarm messages.

*Table 3-26   E100T-G Port-Level Indicators*

| Port-Level Indicators | Description |
|---|---|
| A (Yellow) LED | The port is active. Data is being received and/or transmitted. By default, the LED marked A indicates that the transmitter is active, but it could also be changed in this register to indicate link status, duplex status, or an active receiver. |
| L (Green) LED | Link is established. By default, the LED marked L indicates that the link for this port is up, but it can also be programmed to indicate duplex status, operating speed, or collision. |

## 3.28.3  E100T-G Card Specifications

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 65.00W, 1.35A at –48V, 221.9 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)

- Depth: 228.6 mm (9.000 in.)

- Depth with backplane connector: 235 mm (9.250 in.)

- Weight not including clam shell: 1.0 kg (2.3 lb)

- Compliance

  ONS 15454 SDH cards, when installed in a system, comply with these standards:

  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260

## 3.29  E1000-2-G Card

The E1000-2-G card provides two ports of IEEE-compliant, 1000 MBit/s (Mbps) interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 2 GBits/s (Gbps) per port and 4 GBits/s (Gbps) per card. Each port auto-configures for full duplex and IEEE 802.3x flow control. The E1000-2-G card uses GBIC modular receptacles for the optical interfaces.

Two GBIC modules are offered as separate orderable products for maximum customer flexibility: an IEEE 1000Base-SX compliant, 850-nm optical module and an IEEE 1000Base-LX-compliant, 1300-nm optical module. The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to five kilometers. Other GBIC modules for long-reach 1550-nm and twisted-pair copper will be offered for use with the E1000 card in a future release. Figure 3-49 on page 3-88 shows the card faceplate and Figure 3-50 on page 3-89 shows a block diagram of the card.

**Note**    When using an LX GBIC with 62.5-micron diameter MMF cable, you must install a mode-conditioning patch cord (CAB-GELX-625 or equivalent) between the GBIC and the MMF cable on both the transmit and receive ends of the link. The mode-conditioning patch cord is required for link distances less than 328 feet (100 m) or greater than 984 feet (300 m). The mode-conditioning patch cord prevents overdriving the receiver for short lengths of MMF and reduces differential mode delay for long lengths of MMF.

**Warning**    **Class 1 laser product.**

**Figure 3-49   E1000-2-G faceplate**

**Figure 3-50   E1000-2-G block diagram**



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

The E1000-2-G Gigabit Ethernet card provides high-throughput, low-latency packet switching of Ethernet encapsulated traffic (IP and other Layer 3 protocols) across an SDH/SONET network while providing a greater degree of reliability through SDH/SONET "self-healing" protection services. This enables network operators to provide multiple 1000 MBit/s (Mbps) access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic is provided.

The E1000-2-G card eliminates the need for external aggregation equipment such as Ethernet or ATM switches at the customer site, remote headends or distributed POPs.

Each E1000-2-G card supports standards-based, Layer 2 Ethernet switching between its Ethernet ports and any other Ethernet or SDH/SONET trunk interfaces on the ONS 15454 SDH. The IEEE 802.1Q tag and port-based VLANS logically isolate traffic (typically subscribers). Priority queuing is also supported to provide multiple classes of service. Two queues are provided on card. Queue level is settable from 0 to 7; 0 to 3 and 4 to 7 map.

You can install the E1000-2-G card into any multispeed slot for a total shelf capacity of 20 Gigabit Ethernet ports. Multiple Ethernet cards installed in an ONS 15454 SDH can act as either a single switching entity or as a single switch supporting a variety of SDH/SONET port configurations.

You can create logical SDH/SONET ports by provisioning VC channels to the packet switch entity within an ADM. Logical ports can be created with a bandwidth granularity of VC-4. In a single or multicard configuration, the ONS 15454 SDH can support 1 VC-4-4c, 2 VC-4-2c, or 4 VC-4-1c unstitched VC signal levels and 2 VC-4-2c or 4 VC-4-1c stitched signal levels.

## 3.29.1  E1000-2-G Card-Level Indicators

The E1000-2-G card faceplate has two card-level LED indicators, listed in Table 3-27 on page 3-90.

*Table 3-27    E1000-2-G Card-Level Indicators*

| Card-Level LEDs | Description |
|---|---|
| Red FAIL LED | The red FAIL LED indicates that the card's processor is not ready or catastrophic software failure occurred on the E1000-2-G card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational. |
| Green ACT LED | A green ACT LED provides the operational status of the E1000-2-G. When the ACT LED is green, it indicates that the E1000-2-G card is active and the software is operational. |
| SF LED | Not used |

## 3.29.2 E1000-2-G Port-Level Indicators

The E1000-2-G card also has one bicolor LED per port. When the green LINK LED is on, the linkbeat is detected, meaning an active network cable is installed. When the green LINK LED is off, an active network cable is not plugged into the port. The amber port ACT LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.

## 3.29.3 E1000-2-G Card Specifications

- Environmental
  - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 53.50W, 1.11A at –48V, 182.7 BTU/hr
- Dimensions
  - Height: 321.3 mm (12.650 in.)
  - Width: 18.2 mm (0.716 in.)
  - Depth: 228.6 mm (9.000 in.)
  - Depth with backplane connector: 235 mm (9.250 in.)
  - Weight not including clam shell: 0.9 kg (2.1 lb)
- Compliance

  ONS 15454 SDH optical cards, when installed in a system, comply with these standards:
  - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11
  - Class 1 laser product

# 3.30  G1000-4 Card

The G1000-4 card provides four ports of IEEE-compliant, 1000 MBit/s (Mbps) interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 1 GBits/s (Gbps) or 2 GBits/s (Gbps) bidirectional per port, and 2.5 GBits/s (Gbps) or 5 GBits/s (Gbps) bidirectional per card. Each port auto-negotiates for full duplex and 802.3x flow control. The G1000-4 card uses GBIC modular receptacles for the optical interfaces.

Cisco offers three GBIC modules as separate orderable products for maximum flexibility:

- IEEE 1000Base-SX compliant, 850-nm, optical module
- IEEE 1000Base-LX-compliant, 1300-nm, optical module
- IEEE 1000Base-ZX-compliant, 1550-nm, optical module

The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to ten kilometers. The 1550-nm ZX optics are designed for single-mode fiber and distances of up to eighty kilometers. shows the card faceplate and the block diagram of the card.

**Note**  When using an LX GBIC with 62.5-micron diameter MMF, you must install a mode-conditioning patch cord (CAB-GELX-625 or equivalent) between the GBIC and the MMF cable on both the transmit and receive ends of the link. The mode-conditioning patch cord is required for link distances less than 328 feet (100 m) or greater than 984 feet (300 m). The mode-conditioning patch cord prevents overdriving the receiver for short lengths of MMF and reduces differential mode delay for long lengths of MMF.

**Warning**  **Class 1 laser product.**

*Figure 3-51   G1000-4 faceplate and block diagram*
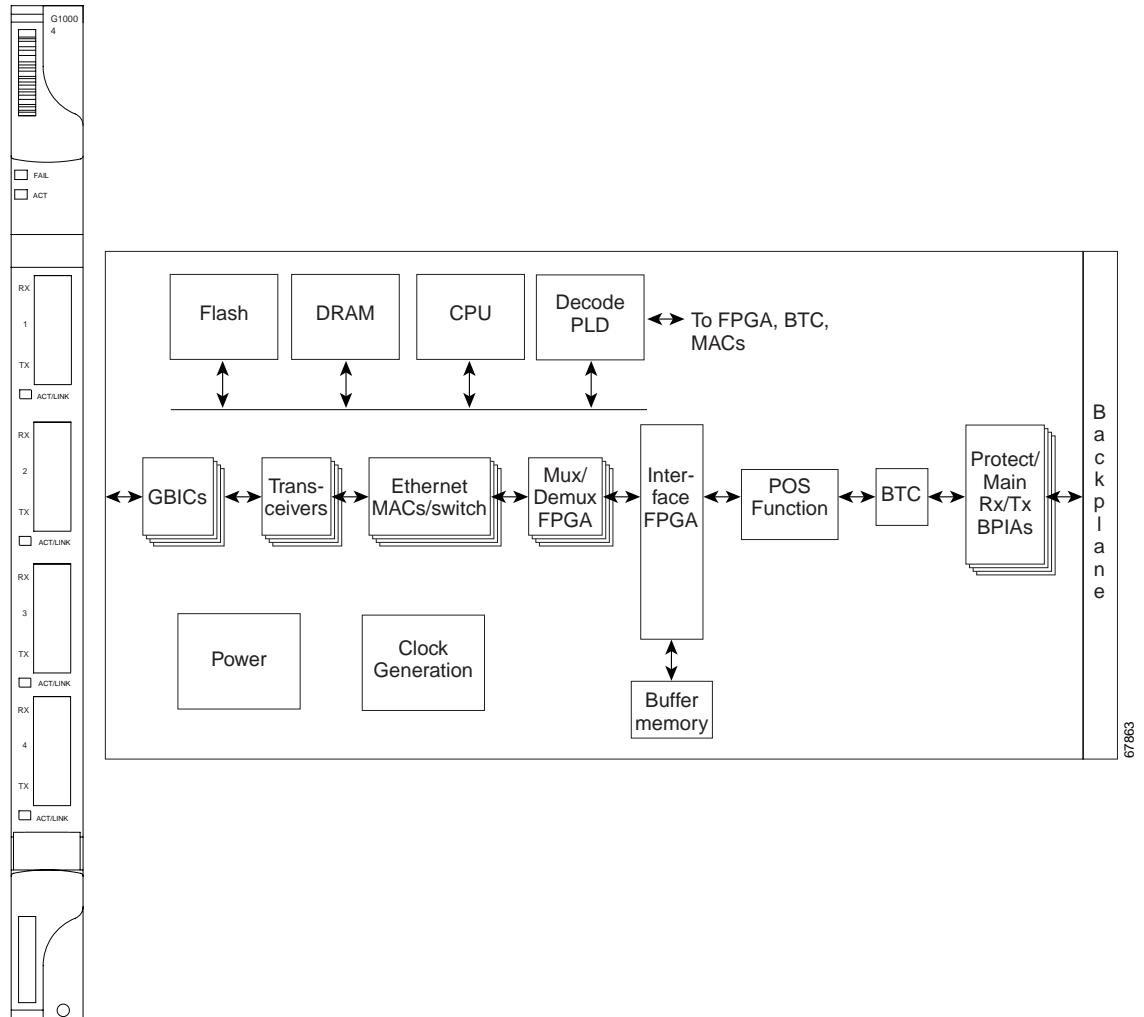


**Warning**   **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

The G1000-4 Gigabit Ethernet card provides high-throughput, low-latency transport of Ethernet encapsulated traffic (IP and other Layer 2 or Layer 3 protocols) across an SDH/SONET network while providing a greater degree of reliability through SDH/SONET "self-healing" protection services. Carrier-class Ethernet transport is achieved by hitless (< 50 ms) performance in the event of any failures or protection switches (such as 1+1 MSP, SNCP, MS-SPRing, or optical equipment protection) and full provisionability and manageability, as in SONET service. Full provisioning support is possible via CTC or CTM.

You can install the G1000-4 card into any multispeed slot for a total shelf capacity of 48 Gigabit Ethernet ports. (The practical limit is 40 ports because at least two slots are typically populated by optical cards such as STM-64). Each G1000-4 card performs completely independently of the other cards in the same shelf.

You can create logical SDH/SONET ports by provisioning VC channels to the packet switch entity within an ADM. Logical ports can be created with a bandwidth granularity of VC-4. In a single or multicard configuration, the ONS 15454 SDH can support 1 VC-4-4c, 2 VC-4-2c, or 4 VC-4-1c unstitched VC signal levels and 2 VC-4-2c or 4 VC-4-1c stitched signal levels. Each Ethernet port can be mapped to exactly one SONET/SDH circuit creating a logical end-to-end Ethernet link over SONET/SDH. The SONET circuit sizes supported are STS-1, STS-3c, STS-6c, STS-9c, STS-24c, and STS-48c.

## 3.30.1  G1000-4 Card-Level Indicators

The G1000-4 card faceplate has two card-level LED indicators, listed in Table 3-28.

*Table 3-28   G1000-4 Card-Level Indicators*

| Card-Level LEDs | Description |
| --- | --- |
| FAIL LED (red) | The red FAIL LED indicates that the card's processor is not ready or a catastrophic software failure occurred on the G1000-4 card. As part of the boot sequence, the FAIL LED is turned on, and it goes off when the software is deemed operational. |
| ACT LED (green) | A green ACT LED provides the operational status of the G1000-4. When the ACT LED is green it indicates that the G1000-4 card is active and the software is operational. |

## 3.30.2  G1000-4 Port-Level Indicators

The G1000-4 card also has one bicolor LED per port. The function of these four LEDs is according to Table 3-29.

*Table 3-29   G1000-4 Port-Level Indicators*

| Port-Level LED | Description |
| --- | --- |
| Off | No link exists to the Ethernet port. |
| Steady amber | A link exists to the Ethernet port, but traffic flow is inhibited. For example, a lack of circuit setup, an error on the line, or a non-enabled port might inhibit traffic flow. |
| Solid green | A link exists to the Ethernet port, but no traffic is carried on the port. |
| Flashing green | A link exists to the Ethernet port, and traffic is carried on the port. The LED flash rate reflects the traffic rate for the port. |

## 3.30.3  G1000-4 Card Specifications

- Environmental
    - Operating temperature: –5 to +45 degrees Celsius (+23 to +113 degrees Fahrenheit)
    - Operating humidity: 5- 95%, noncondensing
    - Power consumption: 63.00W, 1.31A at –48V, 215.1 BTU/hr

- Dimensions

    - Height: 321.3 mm (12.650 in.)

    - Width: 18.2 mm (0.716 in.)

    - Depth: 228.6 mm (9.000 in.)

    - Depth with backplane connector: 235 mm (9.250 in.)

    - Weight not including clam shell: 0.9 kg (2.1 lb)

- Compliance

    ONS 15454 SDH optical cards, when installed in a system, comply with these standards:

    - Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10 and 21 CFR 1040.11

    - Class 1 laser product

CHAPTER 4

# Maintenance

This chapter describes procedures needed to maintain the Cisco ONS 15454 SDH, including:

- Air-filter inspection
- Fan tray replacement
- System software reset and hardware reset (card pull)
- Database backup and restoration
- Card replacement
- Span upgrades
- Fiber cleaning
- Powering down a node
- Powering up a node

*Table 4-1    ONS 15454 SDH Maintenance Tasks*

| Task | Related Procedures |
| --- | --- |
| 4.1 Air Filter Inspection | Inspect and Clean Reusable Air Filter, page 4-3 |
| 4.2 Fan-Tray Assembly | Replace the Fan-Tray Assembly, page 4-4 |
| 4.3 System Reset | Initiate a Software Reset, page 4-6<br>Reset the TCC-I using a Card Pull, page 4-7 |
| 4.4 Database Backup and Restoration | Back Up the Database, page 4-8<br>Restore the Database, page 4-9 |
| 4.5 Restore the Node to Factory Configuration | Use the Reinitialization Tool in Windows, page 4-12<br>Use the Reinitialization Tool in Unix, page 4-14 |

*Table 4-1    ONS 15454 SDH Maintenance Tasks (continued)*

| Task | Related Procedures |
|---|---|
| 4.6 Card Replacement | Replace an In-Service XC10G Card, page 4-17 |
| | Replace a TCC-I Card, page 4-19 |
| | Reset an STM-N Card, page 4-19 |
| | Replace an In-Service STM-N Card in 1+1 Configuration, page 4-20 |
| | Reset an Electrical Card (E1-N-14, DS3i-N-12, or E3-12), page 4-21 |
| | Replace an In-Service Electrical Card (E1-N-14, DS3i-N-12, or E3-12), page 4-22 |
| | Replace an FMEC Card, page 4-23 |
| | Replace an MIC-A/P Card or MIC-C/T/P Card, page 4-23 |
| 4.7 Span Upgrade | Span Upgrade Wizard, page 4-25 |
| | Manually Upgrade a Span on a Two-Fiber MS-SPRing, page 4-31 |
| | Manually Upgrade a Span on a Four-Fiber MS-SPRing, page 4-32 |
| | Manually Upgrade a Span on a 1+1 Group, page 4-33 |
| 4.8 Inspect and Clean Fiber Connectors | Inspect a Fiber Connector, page 4-35 |
| | Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes, page 4-36 |
| | Clean and Scope Fiber Connectors, Using Cletop, page 4-36 |
| | Clean a Fiber Adapter, page 4-37 |
| | Clean a Feedthrough Connector, page 4-37 |
| 4.9 Powering Down a Node | Power Down a Node, page 4-38 |
| 4.10 Powering Up a Node | Power Up a Node, page 4-39 |

# 4.1  Air Filter Inspection

The ONS 15454 SDH contains a reusable filter that you should remove and visually inspect approximately every 30 days, depending on the cleanness of the operating environment. For more information about filter brackets and air filter installation, see Chapter 1 in the *Cisco ONS 15454 SDH Installation and Operations Guide*.

The air filter is made of gray, open-celled, polyurethane foam that is specially coated to provide fire and fungi resistance. Figure 4-1 illustrates a reusable fan tray air filter in an external filter bracket.

If the air filter is inside the fan-tray assembly, go directly to the "Fan-Tray Assembly" Procedure on page 4-4 to remove the fan tray.

*Figure 4-1    Reusable fan tray filter in external filter brackets*



Fan tray filter
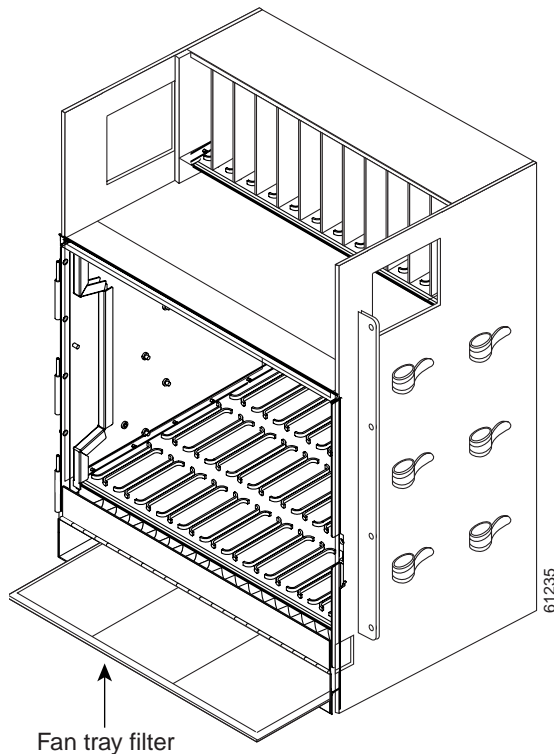
## Procedure: Inspect and Clean Reusable Air Filter

| | |
|---|---|
| **Purpose** | Use this procedure to clean the reusable air filter. |
| **Tools/Equipment** | Vacuum cleaner |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**   Slide the filter out of the external filter brackets. Be careful not to dislodge any dust that could have collected on the filter.

**Step 2**   Visually inspect the filter for dirt and dust.

**Step 3**   If the air filter has a concentration of dirt and dust, vacuum the filter or wash the filter under a faucet with a light detergent.

**Note**   If possible, clean the filter outside of the operating environment to avoid releasing dirt and dust near the equipment.

**Step 4**   If you washed the filter, allow it to air-dry at least 8 hours (or use spare filter).

**Caution**   Do not put a damp filter back in the ONS 15454 SDH.

**Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4**

**Step 5**    Slide the filter to the back of the brackets.

# 4.2 Fan-Tray Assembly

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities. You can remove the fan-tray assembly using the retractable handles and replace it by pushing until it plugs into the receptacle on the back panel.

| | |
|---|---|
| **Purpose** | This procedure replaces an existing FTA with a new FTA. |
| **Tools/Equipment** | Replacement FTA |
| **Prerequisite Procedures** | Procure necessary part number |
| **Onsite/Remote** | Onsite |

⚠
**Caution**    The 15454E-FTA fan-tray assembly can only be installed in ONS 15454 SDH Release 3.1 and later shelf assemblies (15454E-SA-ETSI, part number 800-08708-XX). It includes a pin that does not allow it to be installed in ONS 15454 SDH shelf assemblies released before ONS 15454 Release 3.1. Equipment damage can result from attempting to install the 15454E-FTA-60V or 15454E-FTA-48V in an 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 back panel of the shelf assembly.

✎
**Note**    The 15454-SA-ETSI shelf assembly is required with the ONS 15454 SDH XC10G, OC-192, and OC-48 any slot (AS) cards.

## Procedure: Replace the Fan-Tray Assembly

| | |
|---|---|
| **Purpose** | Use this procedure to replace the fan-tray assembly. |
| **Tools/Equipment** | Pinned hex key |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**    Open the front door of the shelf assembly.

    **a.**  Open the front door lock.

        The ONS 15454 SDH comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

    **b.**  Press the door button to release the latch.

    **c.**  Swing the door open.

**Step 2**    Remove the front door (optional). If you do not want to remove the door, proceed to Step 3.

    **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 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.

⚠

**Caution**    The ONS 15454 SDH system is now without forced-air cooling. The FTA must be placed back in service as quickly as possible to avoid system damage.

**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 any time. For more information on the fan-tray air filter, see the "Air Filter Inspection" section on page 4-2.

**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.

    The fans should start running immediately.

**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, also reattach the ground strap.

**Step 11**    Close and lock the door.

# 4.3  System Reset

You can reset the ONS 15454 SDH TCC-I cards by using the Cisco Transport Controller (CTC) software or by physically resetting a TCC-I card (card pull). A software-initiated reset reboots the TCC-I card and reloads the operating system and the application software. If a card pull is performed, it carries out these tasks and temporarily powers down the TCC-I card, clearing all buffer memory.

You can initiate a software reset for an active TCC-I card or a standby TCC-I card without affecting traffic. But a card pull should only be performed on a standby TCC-I. If you need to pull an active TCC-I card, first you should initiate a software reset on a card to put it into standby mode.

## Procedure: Initiate a Software Reset

| Purpose | Use the CTC software to reset the ONS 15454 SDH. |
|---|---|
| **Tools/Equipment** | Workstation configured for CTC software |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**  Log into the CTC software.

**Step 2**  At the node (default login) view, right-click the TCC-I card to reveal a shortcut menu.

**Step 3**  Click **Reset Card.** (See Figure 4-2).

*Figure 4-2    Resetting from the TCC-I card pull-down menu*
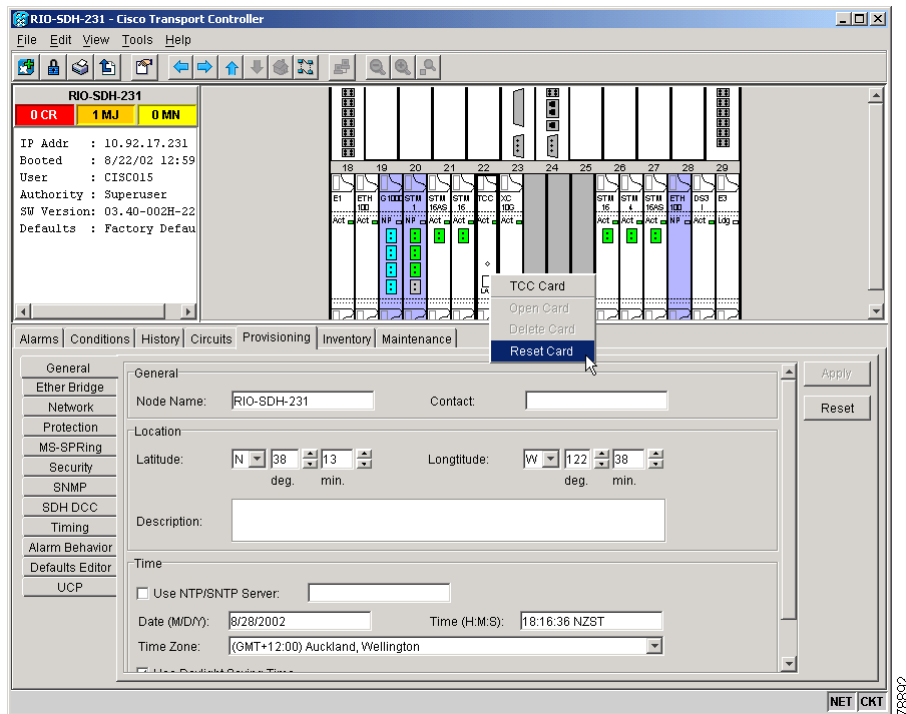


**Step 4**  Click **Yes** in the dialog box when the "Are You Sure?" prompt appears.

**Step 5**  Click **OK** in the dialog box when the "Lost connection to node, changing to Network View" prompt appears.

**Step 6**  Confirm that the TCC-I card is in standby mode after the reset.

- If you are looking at the physical ONS 15454 SDH, the ACT/STBY LED is steadily lit amber.

- If you are looking at the CTC Node view of the ONS 15454 SDH, a yellow LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

## Procedure: Reset the TCC-I using a Card Pull

| | |
|---|---|
| **Purpose** | Reset TCC-I card physically by removing and reseating card |
| **Tools/Equipment** | Workstation configured for CTC software |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

⚠
**Caution**  Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

⚠
**Caution**  During the reboot period, there is no TCC-I redundancy.

✎
**Note**  To determine whether the TCC-I card is in active mode or standby mode, view it in the CTC software and position the cursor over the TCC-I card graphic to display the status.

**Step 1**  If you need to perform a card pull on an active TCC-I card, initiate a software reset on the active TCC-I card first. (See the "Initiate a Software Reset" Procedure on page 4-6.)

**Step 2**  When the TCC-I is in standby mode, unlatch the top and bottom ejector levers on the TCC-I card.

**Step 3**  Pull the card outward from the slot until the lighted LEDs turn off.

**Step 4**  Wait 30 seconds. Reinsert the card and close the ejector levers.

✎
**Note**  The TCC-I card takes several minutes to reboot and display the amber standby LED after rebooting.

✎
**Note**  During bootup of the reinserted TCC-I card, the FMEC cards in the system will not be visible in the CTC software. They will be visible in the software again after the TCC-I card has finished booting.

✎
**Note**  When a second TCC-I card is inserted into the shelf, it will synchronize its software, its backup software, and its database with the active TCC-I. If its software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy from the active TCC-I. This copying will take about 15 to 20 minutes. If its backup software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy the backup software from the active TCC-I. This copying, again, will take about 15 to 20 minutes. Copying the database from the active TCC-I will take about 3 minutes. So, depending on the software existing in the new TCC-I, booting it up will take between 3 and about 40 minutes.

# 4.4  Database Backup and Restoration

When dual TCC-I cards are installed in the ONS 15454 SDH, each TCC-I card hosts a separate copy of the database. If the working TCC-I card database fails, the protect card database is available. You can store a backup version of the database on a CTC software workstation. This off-system storage should be part of regular ONS 15454 SDH maintenance at approximately weekly intervals. It should also be performed to prepare an ONS 15454 SDH for disasters.

**Note**    E100T-G cards lose traffic for approximately 30 seconds when an ONS 15454 SDH database is restored. The CARLOSS alarm appears and clears during this process. The traffic outage happens during the spanning-tree reconvergence.

**Note**    If you are restoring the database on multiple nodes, wait five minutes between each database restoration.

**Note**    The following parameters are not backed up and restored: node name, IP address, mask and gateway, and IIOP port. If you change the node name and then restore a backed-up database with different node names, the circuits will map to the new node name. Cisco recommends keeping a record of the old and new node names.

## Procedure: Back Up the Database

| | |
|---|---|
| **Purpose** | This procedure backs up an ONS 15454 SDH database. |
| **Tools/Equipment** | Workstation configured for CTC software |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Note**    It is advisable to perform a backup when a node is first installed, so that the node can be restored to factory configuration if necessary. For that procedure, see the "Restore the Node to Factory Configuration" section on page 4-11.

**Step 1**    Log into the CTC software.

**Step 2**    Click the **Maintenance > Database** tabs (Figure 4-3 on page 4-9).

*Figure 4-3    Backing up the TCC-I card database*
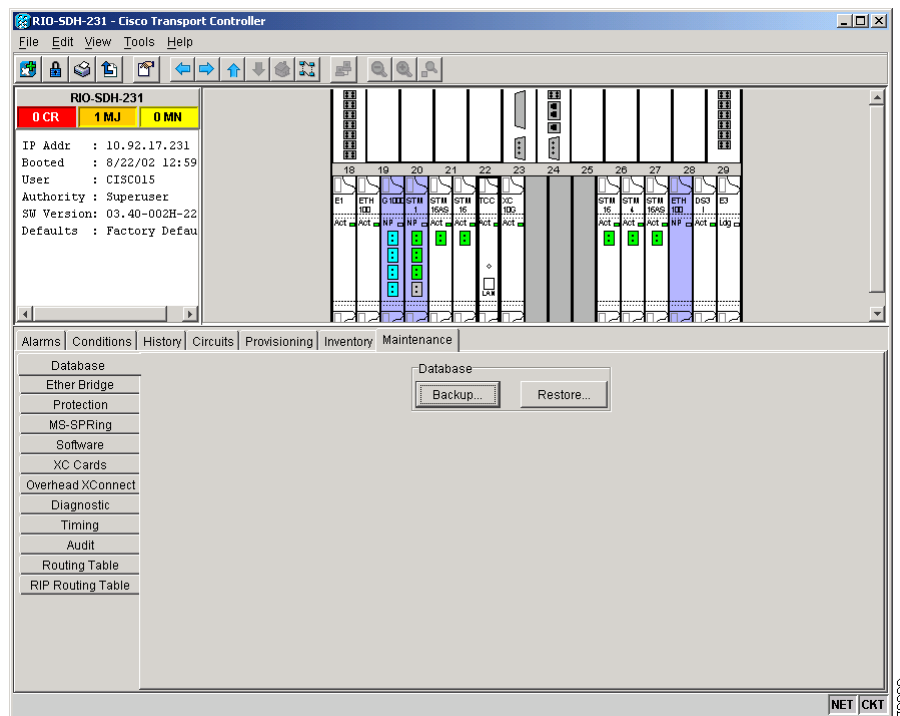


**Step 3**    Click **Backup**.

**Step 4**    Navigate to a workstation hard drive or network storage location.

**Step 5**    Enter a file name in the File Name field. It is recommended to use the file extension .db.

**Step 6**    Click **Save** and wait while database is backed up.

**Step 7**    Click OK to confirm successful completion of the database backup (Figure 4-4).

*Figure 4-4    Confirming a database backup is complete*
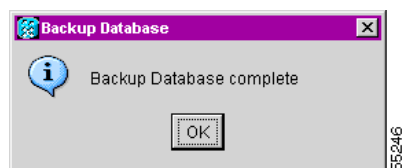


# Procedure: Restore the Database

| | |
|---|---|
| **Purpose** | Restoring the data base of a node |
| **Tools/Equipment** | Workstation configured for CTC software |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**  Log into the CTC software.

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

**Step 3**  Click **Restore** (Figure 4-3).

**Step 4**  Locate the database file stored on the workstation hard drive or in the network storage area.

**Step 5**  Click the database file to highlight it.

The file probably has a .db extension.

**Step 6**  Click **Open.** The DB Restore dialog box (Figure 4-5) appears.

> ⚠️
>
> **Caution**    Traffic will be affected when you restore a local database from another node.

*Figure 4-5    Restoring the database—Traffic loss warning*
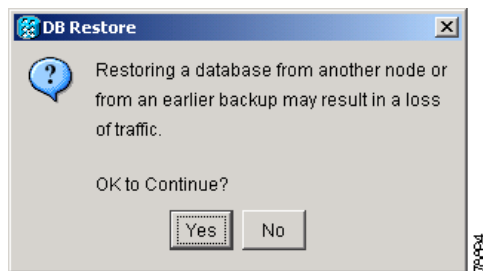


**Step 7**  Click **Yes**. The Restore Database dialog box (Figure 4-6) monitors the file transfer.

*Figure 4-6    Restoring the database—In-process notification*
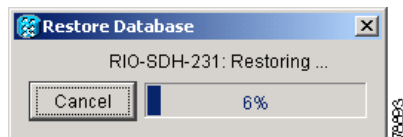


**Step 8**  Wait for the selected file to be completely transferred to the TCC-I card.

> ✎
>
> **Note**    The node will reboot after the files are transferred to the TCC-I.

**Step 9**  Click **OK** in the dialog box when the "Lost connection to node, changing to Network View" prompt appears. Wait for the node to reconnect.

> ✎
>
> **Note**    Any provisioning that took place after the database backup will have to be reconstructed.

# 4.5 Restore the Node to Factory Configuration

| | |
|---|---|
| **Purpose** | Use this procedure to initiate a process that will automatically load and activate a software package and restore the database from a database backup file that was obtained at the time of installation. This process is performed with the RE-INIT.jar utility, also called the reinitialization (reinit) tool. |
| **Tools/Equipment** | CD containing the software, the node's NE defaults, and the reinitialization tool. JRE 1.3.1_02 must also be installed on the computer you will use to perform this procedure. |
| **Prerequisite Procedures** | Back Up the Database, page 4-8 and the backup file which was obtained at installation |
| **Onsite/Remote** | Onsite (if you are replacing a TCC-I card) or remote |

⚠️

**Caution**    If you are restoring the database on multiple nodes, wait until the TCC-I cards have rebooted on each node before proceeding to the next node.

⚠️

**Caution**    Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you only use the Search Path field. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

✎

**Note**    If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 4-7 on page 4-12).

✎

**Note**    The following parameters are not backed up and restored: node name, IP address, mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

**Step 1**    If you need to install or replace one or more TCC-I cards, see the *Cisco ONS 15454 SDH Installation and Operations Guide* or the "Replace a TCC-I Card" task on page 4-19.

**Step 2**    If you are using Microsoft Windows, complete the "Use the Reinitialization Tool in Windows" task on page 4-12.

**Step 3**    If you are using UNIX, complete the "Use the Reinitialization Tool in Unix" task on page 4-14.

You can use the reinitialization tool to upload the software package, restore the node's database, or both by checking the appropriate fields shown below in Figure 4-7. The default setting for this tool is shown with both upload package (software) and restore database selected.

## Procedure: Use the Reinitialization Tool in Windows

| | |
|---|---|
| **Purpose** | This procedure describes how to use the reinitialization tool in Windows. Use this tool to upload the software package and/or restore the database after it has been backed up. |
| **Tools/Equipment** | CD containing the desired software version and the reinitialization tool |
| **Prerequisite Procedures** | Back Up the Database, page 4-8 |
| **Onsite/Remote** | Onsite or remote |

**Note** The TCC-I cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

**Step 1** Insert the system software CD containing the reinitialization tool (Figure 4-7) into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

**Step 2** To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.

**Step 3** On the CD drive, go to **CISCO15454** folder and double-click the **RE-INIT.jar** file to open the reinitialization tool (Figure 4-7).

**Step 4** Depending on what file(s) you wish to restore, perform the following:

- To upload the software package and the database from the same directory, go to Step 5.
- To restore the database, go to Step 6.
- To upload the software, go to Step 7.

*Figure 4-7    Reinitialization tool in Windows*



**Step 5** To automatically upload both the software package and the database from the same directory, perform the following steps:

**a.** If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

**b.** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-7).

**c.** Verify that the Re-Init Database, Upload Package, and Confirm checkboxes are checked.

**d.** In the Search Path field, direct this tool to the directory where the backed up database and software package are located by typing the entire path, or use the Browse button to browse for the file. If the software package and database you want to upload is in the same directory as the RE-INIT.jar file you opened, the Search Path field already contains the correct path to the files.

⚠️

**Caution**    Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

**e.** Click **Go**. The reinitialization tool then looks for the appropriate product-specific software package files and database that is backed up in the specified location.

⚠️

**Caution**    Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

**f.** A confirmation dialog box opens (Figure 4-8). Click **Yes** to upload the database you specified. You should be sure you are uploading the correct database before you proceed.

**g.** The status bar at the bottom of the screen will display Complete when the software upload and database restore processes are completed.

**h.** Verify that the NE default settings in CTC match the settings found on the CD.

*Figure 4-8    Confirm NE Restoration*
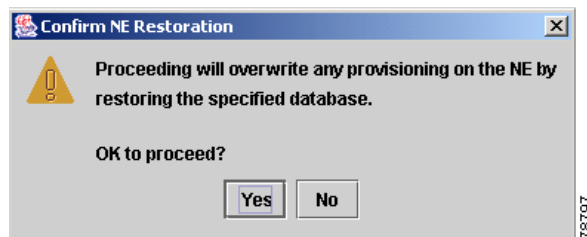


**Step 6**    To restore only the database using the reinitialization tool, perform the following steps:

**a.** If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

**b.** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-7).

**c.** Verify that the Re-Init Database and Confirm checkboxes are checked and Upload Package is unchecked.

**d.** In the Database field, direct this tool to the directory where the backed up database files and software package are located by typing the entire path, or use the Browse button to browse for the file. (The network element defaults are also contained in the database.)

**e.** Click **Go**. The reinitialization tool then looks for the appropriate product-specific database file that is backed up in the specified location.

**f.** A confirmation dialog box opens (Figure 4-8). Click **Yes**.

**g.** The status bar at the bottom of the screen will display Complete when the restore database process is complete.

**Step 7** To upload only the software package using the reinitialization tool, perform the following steps:

    **a.** If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

    **b.** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-7 on page 4-12).

    **c.** Verify that the Upload Package and Confirm checkboxes are checked and Re-Init Database is unchecked.

    **d.** Direct this tool to the location where the latest software package files are located by typing the entire path in the Package field.

    **e.** Click **Go**. The reinitialization tool then looks for the appropriate product-specific software package files in the specified location.

    **f.** A confirmation dialog box opens (Figure 4-8 on page 4-13). Click **Yes**.

    **g.** The status bar at the bottom of the screen will display Complete when the software upload process is complete.

**Step 8** Manually set the node name and network configuration to site-specific values. See the *Cisco ONS 15454 SDH Installation and Operations Guide* for procedures to set the name, date, time, and contact information as well as the node name, IP address, mask and gateway, and IIOP port.

## Procedure: Use the Reinitialization Tool in Unix

| | |
|---|---|
| **Purpose** | This procedure describes how to use the reinitialization tool in a UNIX environment. Use this tool to upload the software package and/or restore the database after it has been backed up. |
| **Tools/Equipment** | CD containing the desired software version and the reinitialization tool |
| **Prerequisite Procedures** | Back Up the Database, page 4-8 |
| **Onsite/Remote** | Onsite or remote |

**Note** The TCC+ cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

**Step 1** Insert the system software CD containing the software package and the reinitialization tool (Figure 4-9 on page 4-15) into the UNIX workstation. If the CTC Installation Wizard opens, click **Cancel**.

**Step 2** To find the recovery tool file, go to the CISCO15454 directory on the CD (usually `/cdrom/cdrom0/CISCO15454`).

**Step 3** If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinitialization tool (Figure 4-9 on page 4-15). If you are working with a command line interface, run `java -jar RE-INIT.jar`.

***Figure 4-9    The reinitialization tool in UNIX***



**Step 4**    Depending on what file(s) you wish to restore, perform the following:

- To upload the software package and the database from the same directory, go to Step 5.

- To restore the database, go to Step 6.

- To upload the software, go to Step 7.

**Step 5**    To upload both the software package and the database from the same directory, perform the following steps:

   **a.**   If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

   **b.**   Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-9).

   **c.**   Verify that the Re-Init Database, Upload Package, and Confirm checkboxes are checked.

   **d.**   In the Search Path field, direct this tool to the directory where the backed up database file and software package are located by typing the entire path, or use the Browse button to browse for the file. If the software package and database you want to upload is in the same directory as the RE-INIT.jar file you opened, the Search Path field already contains the correct path to the files.

   ⚠
   **Caution**    Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

   If you upload the NE defaults database instead of a backed-up database, you will eliminate any existing provisioning on the node (including circuits and timing).

   **e.**   Click **Go**. The reinitialization tool then looks for the appropriate product-specific software package files and database that is backed up in the specified location.

   **f.**   A confirmation dialog box opens (Figure 4-8 on page 4-13). Click **Yes**.

   **g.**   The status bar at the bottom of the screen will display Complete when the process has completed.

   **h.**   Verify that the NE default settings in CTC match the settings found on the CD.

**Step 6**   To restore only the database s using the reinitialization tool, perform the following steps:

a. If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

b. Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-9 on page 4-15).

c. Verify that the Restore Database and Confirm checkboxes are checked.

d. Direct this tool to the directory where the backed up database files are located by typing the entire path in the Database field.

e. Click **G**o. The reinitialization tool then looks for the appropriate product-specific database file that is backed up in the specified location.

f. A confirmation dialog box opens (Figure 4-8 on page 4-13). Click **Yes**.

g. The status bar at the bottom of the screen will display Complete when the Upload Package process is complete.

**Step 7**   To restore only the database using the reinitialization tool, perform the following steps:

a. If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

b. Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-9 on page 4-15).

c. Verify that the Re-Init Database and Confirm checkboxes are checked and Upload Package is unchecked.

d. In the Database field, direct this tool to the directory where the backed-up database files and software package are located by typing the entire path, or use the Browse button to browse for the file.

e. Click **Go**. The reinitialization tool then looks for the appropriate product-specific database file that is backed up in the specified location.

f. A confirmation dialog box opens (Figure 4-8 on page 4-13). Click **Yes**.

g. The status bar at the bottom of the screen will display Complete when the restore database process is complete.

**Step 8**   To upload only the software package using the reinitialization tool, perform the following steps:

a. If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

b. Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 4-9 on page 4-15).

c. Verify that the Upload Package and Confirm checkboxes are checked and Re-Init Database is unchecked.

d. Direct this tool to the location where the latest software package files are located by typing the entire path in the Package field.

e. Click **Go**. The reinitialization tool then looks for the appropriate product-specific software package files in the specified location.

f. A confirmation dialog box opens (Figure 4-8 on page 4-13). Click **Yes**.

g. The status bar at the bottom of the screen will display Complete when the Upload Package process is complete.

Step 9    Manually set the node name and network configuration to site-specific values. See the *Cisco ONS 15454 SDH Installation and Operations Guide* for procedures to set the name, date, time, and contact information as well as the node name, IP address, mask and gateway, and IIOP port.

# 4.6  Card Replacement

Cards can be replaced with the same type of card or with a different type.

- To replace an ONS 15454 SDH card with another card of the same type, you do not need to change the database. Pull the old card and replace it with a new one.

- To replace a card with a different type of card, pull the card and replace it with a new one. Then delete the original card in the CTC software.

**Note**    An improper removal (IMPROPRMVL) alarm occurs whenever a card pull is performed unless the card is deleted in the CTC software first. The alarm will clear after the card replacement is complete.

**Caution**    Always use an ESD wristband when working with an ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the mid-right outside of the shelf assembly.

**Note**    Traffic can be interrupted when you pull an active card from the ONS 15454 SDH. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If an active card needs to be replaced, switch it to standby mode as shown in the "Replace an In-Service XC10G Card" section on page 4-17, the "Replace an In-Service STM-N Card in 1+1 Configuration" section on page 4-20, or the "Replace an In-Service Electrical Card (E1-N-14, DS3i-N-12, or E3-12)" section on page 4-22, before pulling the card from the node.

## Procedure: Replace an In-Service XC10G Card

| | |
|---|---|
| **Purpose** | Replacing an in-service XC10G card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Caution**    Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

**Note**    Resetting an XC10G card can cause a linear 1+1 STM-N protection switch or an MS-SPRing protection switch.

**Note** Traffic can be interrupted when you pull an active card from the ONS 15454 SDH. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If an active card needs to be replaced, follow the procedure to switch the XC10G card to standby mode before you pull the card from the node.

**Step 1** Take these precautions before initiating an XC10G card reset to avoid causing a linear 1+1 or MS-SPRing protection switch.

  **a.** Ensure that the working span is active on the local and remote nodes.

  **b.** Ensure that the working span is carrying error-free traffic without SD alarms or SF alarms.

  **c.** Place a lockout on the protection span before initiating an XC10G reset. (For information about placing lockouts, refer to the *ONS 15454 SDH Installation and Operations Guide*.) In an MS-SPRing, place a lockout on the East and West node cards adjacent to the XC10G switch node. For example, if you are switching the XC10G on Node B, place a lockout on the Node A West card and on the Node C East card. You do not need to place lockouts on Node B.

    <------East [Node A] West------East [Node B] West------East [Node C] West------>

    Before setting the lockout, verify that the MS-SPRing is not switched. Traffic can be lost if the MS-SPRing is switched when the lockout is set. In a 1+1 protection scheme, place a lockout on the protect card and verify that traffic is traveling over the working span before setting the lockout.

**Step 2** Determine which XC10G card is active. The active card ACT/STBY LED is green. The standby card ACT/STBY LED is yellow.

**Note** You can determine whether the XC10G card is in active mode or standby mode by viewing it in the CTC software and positioning the cursor over the XC10G card graphic to display the status.

If the card to be replaced is already standby, go to Step 4.

**Step 3** Switch the active XC10G card to standby.

  **a.** In the node view, click the **Maintenance > XC Cards** tabs.

  **b.** In the Cross Connect Cards area, click **Switch**.

  **c.** Click **Yes** on the Confirm Switch dialog box.

**Note** After the active XC10G goes into standby mode, the original standby slot becomes active. This causes the former standby card ACT/STBY LED to become green.

**Step 4** Pull the standby XC10G card from the ONS 15454 SDH.

**Step 5** Insert the replacement XC10G card into the empty slot. The replacement card boots up and becomes ready for service after approximately one minute.

**Step 6** Release the protection lockouts.

## Procedure: Replace a TCC-I Card

| | |
|---|---|
| **Purpose** | Replacing a TCC-I card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

⚠️

**Caution**    Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

**Step 1**    Prepare according to the "Reset the TCC-I using a Card Pull" Procedure on page 4-7.

**Step 2**    Pull the TCC-I card to be replaced from the ONS 15454 SDH.

**Step 3**    Insert the replacement TCC-I card into the empty slot. The replacement card boots up and becomes ready for service after about three to forty minutes.

✎

**Note**    When a second TCC-I card is inserted into the shelf, it will synchronize its software, its backup software, and its database with the active TCC-I. If its software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy from the active TCC-I. This copying will take about 15 to 20 minutes. If its backup software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy the backup software from the active TCC-I. This copying, again, will take about 15 to 20 minutes. Copying the database from the active TCC-I will take about 3 minutes. So, depending on the software existing in the newly inserted TCC-I, booting it up will take between 3 and about 40 minutes.

## Procedure: Reset an STM-N Card

| | |
|---|---|
| **Purpose** | Resetting an STM-N card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

✎

**Note**    An STM-N reset can cause a linear 1+1 STM-N protection switch or an MS-SPRing protection switch.

✎

**Note**    For optical cars in 1+1 configurations, there will be an active card and a standby card. For SNCP and MS-SPRing configurations, both STM-N cards will be active. Traffic will be interrupted on SNCPs and MS-SPRings if you reset a traffic-bearing card with protection switching disabled.

✎

**Note**    The STM-N card should be replaced if a red FAIL LED appears.

**Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, R3.4**

**Warning**    **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

**Warning**    **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Step 1**    If the card to be reset is a standby card, right-click the card and choose **Reset Card** from the shortcut menu.

If the card is not standby, go to Step 2.

**Step 2**    To avoid causing a linear 1+1 or MS-SPRing protection switch, ensure that the working span is active on the local and remote nodes.

**Step 3**    Ensure that the working span is carrying error-free traffic without FAIL alarms or SF alarms.

**Step 4**    Perform a lockout on the protection span  in the CTC software before initiating an STM-N card reset. In an MS-SPRing, place a lockout on the East and West node cards adjacent to the XC10-G switch node. For example, if you are switching the XC10-G on Node B, place a lockout on the Node A West card and on the Node C East card.

<------East [Node A] West------East [Node B] West------East [Node C] West------>

You do not need to place lockouts on Node B. Before setting the lockout, verify that the MS-SPRing is not switched. Traffic can be lost if the MS-SPRing is switched when the lockout is set. In a 1+1 protection scheme, place a lockout on the protect card and verify that traffic is traveling over the working span before setting the lockout.

## Procedure: Replace an In-Service STM-N Card in 1+1 Configuration

| | |
|---|---|
| **Purpose** | Replacing an in-service STM-N card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Caution**    Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

**Step 1**    In the CTC software, determine which STM-N card is active.

A green LED indicates an active card. A yellow LED indicates a standby card.

**Note**    You can determine whether the card is in active mode or standby mode by viewing it in the CTC software and positioning the cursor over the card graphic to display the status.

**Step 2**    Switch the active STM-N card to standby.

    **a.**    In the node view, right-click the STM-N card.

    **b.**    Select **Reset Card** from the shortcut menu.

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

**Note**    After the working STM-N card goes into protection, the protection slot becomes working. This causes the former working card ACT LED to switch off.

**Step 3**    Pull the standby STM-N card from the ONS 15454 SDH.

**Step 4**    Insert the replacement STM-N card into the empty slot. The replacement card boots up and becomes ready for service after approximately one minute. After this procedure, the card is ready  for protection function.


## Procedure: Reset an Electrical Card (E1-N-14, DS3i-N-12, or E3-12)

| | |
|---|---|
| **Purpose** | Resetting an electrical card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Note**    An  electrical card reset can cause a 1:1 or 1:N protection switch.

**Note**    Traffic can be interrupted if you pull an active card from the ONS 15454 SDH. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If an active card needs to be replaced, follow the procedure to switch the electrical card to standby mode before you pull the card from the node.

**Note**    The cards should be replaced when the red FAIL LED appears.

Take these precautions before performing an electrical card reset to avoid causing a 1:1 or 1:N protection switch.

**Step 1**    If the card to be reset is a standby card, right-click the card and choose **Reset Card** from the shortcut menu.

If the card is not standby, go to Step 2.Ensure that the working span is active on the local and remote nodes.

**Step 2**    Ensure that the working span is carrying error-free traffic without FAIL or SF alarms.

**Step 3**    Place a lockout on the protection span before initiating an electrical card reset. In an MS-SPRing, place a lockout on the East and West cards of the nodes adjacent to the electrical card switch node; for example, to switch the electrical card on Node B, place the lockout on the West card of Node A and on the East card of Node C. No lockout is necessary on Node B.

<------East [Node A] West------East [Node B] West------East [Node C] West----->

Before the lockout is set, verify that the MS-SPRing is not switched. Traffic can be lost if a lockout is set when the MS-SPRing is switched.In a 1:1 protection scheme, place a lockout on the protect card and verify that traffic is traveling over the working span before setting the lockout.

## Procedure: Replace an In-Service Electrical Card (E1-N-14, DS3i-N-12, or E3-12)

| | |
|---|---|
| **Purpose** | Replacing an in-service electrical card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

⚠

**Caution**   Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

**Step 1**   Determine which electrical card is active.

The active card ACT/STBY LED is green. The standby card ACT/STBY LED is yellow.

✎

**Note**   You can determine whether the card is in active mode or standby mode by viewing it in the CTC software and positioning the cursor over the card graphic to display the status.

**Step 2**   Switch the active card to standby.

   **a.**   In the node view, click the **Maintenance > Protection** tabs.

   **b.**   Under Protection Groups, click the protection group containing the card to be replaced.

   **c.**   Under Selected Group, click the Working/Active card and click **Switch**.

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

✎

**Note**   A minor alarm appears on the manually switched slot. After the active electrical card goes into standby, the original standby slot becomes active. This causes the former standby card ACT/STBY LED to become green.

**Step 3**   Pull the standby card from the ONS 15454 SDH.

**Step 4**   Insert the replacement card into the empty slot. The replacement card boots up and becomes ready for service after approximately one minute. Release the protection switch:

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

   **b.**   Under Protection Groups, click the group containing the card to be released.

   **c.**   Under Selected Group, click the Protect/Active card.

   **d.**   Click **Clear**.

## Procedure: Replace an FMEC Card

| | |
|---|---|
| **Purpose** | Replacing an FMEC card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

⚠️
**Caution**    Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

✎
**Note**    Traffic will be interrupted if active FMEC (E1, E3/DS3, DS1/E1) cards are removed from the ONS 15454 SDH.

**Step 1**    Disconnect all the cables with 1.0/2.3 miniature coax connectors from the damaged FMEC card.

✎
**Note**    To disconnect the cable from the FMEC, pull the ring of the connector using the coaxial removal tool.

**Step 2**    Pull the damaged FMEC card from the shelf assembly.

**Step 3**    Insert the replacement FMEC card into the empty slot.

**Step 4**    Reposition the cables. Gently push the cable connector down until the cable connector slides into the FMEC connector with a click.

The replacement card is now ready for traffic. The traffic starts automatically.

## Procedure: Replace an MIC-A/P Card or MIC-C/T/P Card

| | |
|---|---|
| **Purpose** | Replacing an MIC-A/P or MIC-C/T/P card |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

⚠️
**Caution**    Hazardous voltage or energy may be present on the backplane when the system is operating. Use caution when servicing.

✎
**Note**    Pulling an active MIC-A/P card or MIC-C/T/P card from the ONS 15454 SDH causes alarms. Traffic is affected if an active MIC-A/P card or an active MIC-C/T/P card is replaced while there is no redundant power supply.

**Step 1**    Disconnect the cable from the damaged MIC-A/P card or MIC-C/T/P card.

> ✎
> **Note** To disconnect the cable from the FMEC, pull the ring of the connector using the coaxial removal tool.

**Step 2** Pull the damaged MIC-A/P card or MIC-C/T/P card from the shelf assembly.

**Step 3** Insert the replacement MIC-A/P card or MIC-C/T/P card into the empty slot.

**Step 4** Gently push the cable with the 1.0/2.3 miniature coax connector down until the cable connector slides into the 1.0/2.3 miniature coax connector with a click.

**Step 5** Gently push the other cable connector down until the cable connector slides into the 1.0/2.3 miniature coax connector. The replacement card is ready for operation.

> ✎
> **Note** For proper system operation, both the MIC-A/P card and the MIC-C/T/P card must be installed in the shelf.

# 4.7  Span Upgrade

A span includes the set of optical fiber ("lines") between two ONS 15454 SDH nodes. A span upgrade raises the STM-N signal transmission rate of all the lines constituting the spans. It is done by coordinated line upgrades that move traffic from lower-rate optical card(s) to higher-rate optical card(s). No other span attributes are changed.

Only single-port cards can be upgraded. You can upgrade the following ONS 15454 SDH cards in an in-service span:

- STM-4 to STM-16
- STM-4 to STM-64
- STM-16 to STM-64

When a span is upgraded, the higher-rate line card must replace the lower-rate card in the same slot. If the spans to be upgraded are part of a ring topology, all spans in the ring must be upgraded. The protect configuration (two-fiber MS-SPRing, four-fiber MS-SPRing, or 1+1) that was used with lower-rate optical card is retained in the higher-rate upgrade.

Span upgrades can be performed using the CTC software upgrade wizard, or they can be performed manually. To use the wizard, follow the procedure in the "Span Upgrade Wizard" section. To upgrade a span manually, follow the procedures in the "Manual Span Upgrades" section.

> ✎
> **Note** Span upgrades do not change SDH topologies. For example, a 1+1 scheme is not upgraded to a two-fiber MS-SPRing during a span upgrade. See the SDH Topologies chapter in the *Cisco ONS 15454 SDH Installation and Operations Guide* for topology upgrade procedures.

# 4.7.1  Span Upgrade Wizard

The Span Upgrade Wizard automates all steps in the manual span upgrade procedure (MS-SPRing and 1+1). The Wizard can upgrade both lines on one side of a four-fiber MS-SPRing or both lines of a 1+1 group. The Wizard upgrades MSPs and two-fiber MS-SPRings one line at a time. The Span Upgrade Wizard requires that spans have DCC enabled.

**Note**  The CTC software Span Upgrade Wizard only supports STM-N span upgrades. It does not support electrical card upgrades.

**Note**  During the span upgrade, minor alarms and conditions will occur and clear automatically. However, no service-affecting alarms (SA, Major, or Critical) should be expected. If any service-affecting alarms occur, Cisco recommends backing out of the procedure.

## Procedure: Span Upgrade Wizard

| | |
|---|---|
| **Purpose** | Upgrading a span |
| **Tools/Equipment** | STM cards that support the new line rate |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Note**  If an abnormal error occurs while you are using the Span Upgrade Wizard, you must exit the wizard and initiate the manual procedure to finish the upgrade, or you must back out of the procedure. If you continue the upgrade manually, examine the standing conditions and alarms to identify the stage where the wizard failure occurred.

**Note**  If you are upgrading a 1+1 group, upgrade the protect line first, regardless of which line is active.

**Note**  You cannot downgrade if circuits exist on the STM-Ns that would be removed (i.e., the higher STM-Ns).

**Step 1**  Ensure no alarms or conditions are present on the span to be upgraded. An unresolved alarm or condition will likely cause the wizard to fail.

**Step 2**  In the network view, right-click the span to be upgraded.

**Step 3**  Choose **Span Upgrade** from the shortcut menu (Figure 4-10 on page 4-26).

**Note**  If the Span Upgrade option does not appear when you right-click the span, it cannot be upgraded.

*Figure 4-10   Span upgrade on shortcut menu*
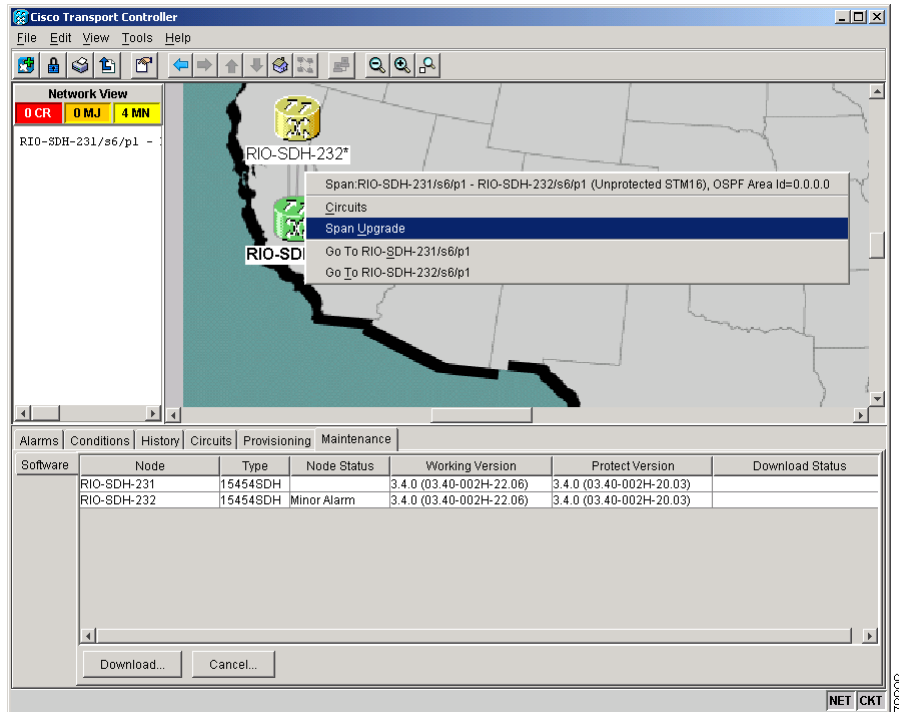


A Span Upgrade Dialog box appears showing Step 1 of the wizard (Figure 4-11).

*Figure 4-11    Beginning the Span Upgrade wizard*
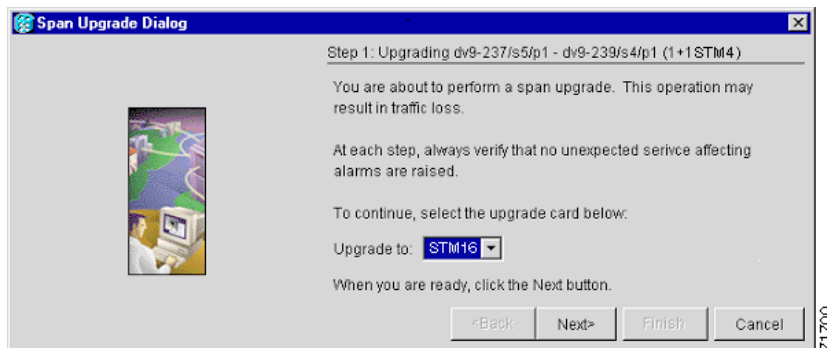


**Step 4**   Select the upgrade card from the pull-down menu and click **Next**. A Span Upgrade Dialog box appears showing Step 2 of the wizard (Figure 4-12 on page 4-27).

*Figure 4-12   Sending a force switch command*
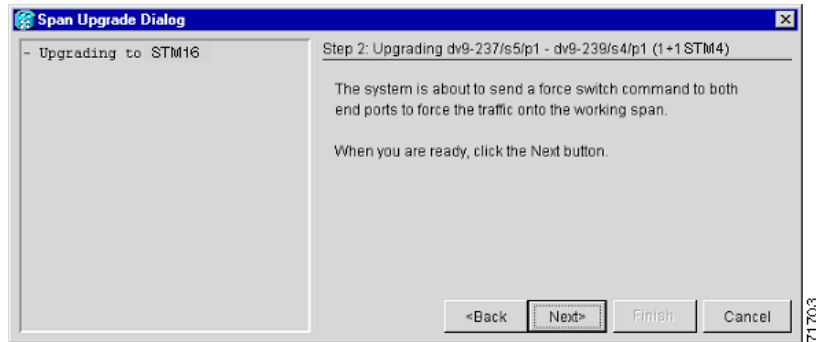


**Step 5**    Click **Next** to send a force switch command, forcing the traffic onto the working lines. Or, click **Back** to return to the previous dialog box. A Span Upgrade Dialog box appears showing Step 3 of the wizard (Figure 4-13).

**Note**      This is the only step in the Span Upgrade Wizard that has the **Back** button enabled.

*Figure 4-13   Waiting for a force switch command to take effect*
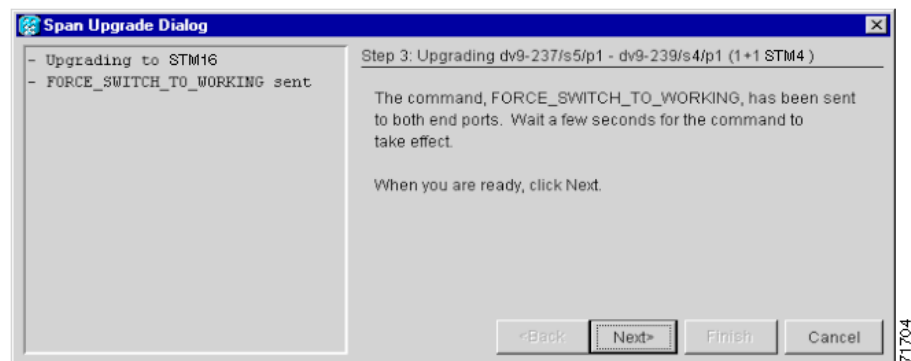


**Step 6**    Wait 5 to 10 seconds for the command to take effect and click **Next**. An error dialog box appears if more time is needed. A Span Upgrade Dialog box appears showing Step 4 of the wizard (Figure 4-14 on page 4-28).

*Figure 4-14   Removing the STM-N cards from the protect slots*
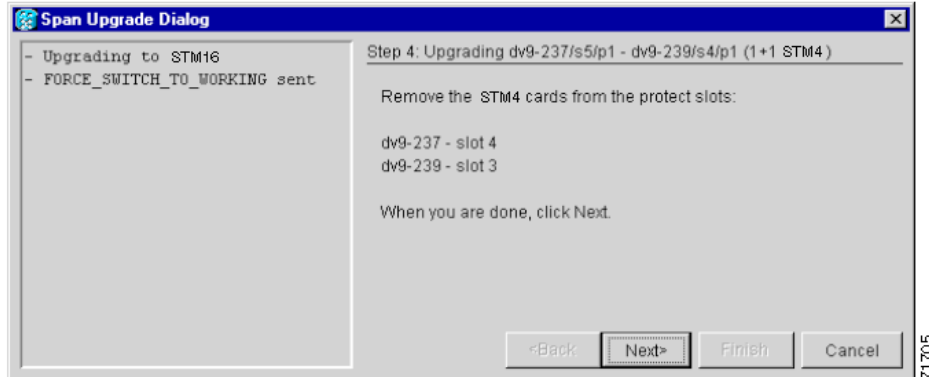


Step 7    Remove the fiber from the lower-rate card and ensure that traffic is still running.

Step 8    Remove the lower-rate STM-N cards from the protect slots and click **Next**. A Span Upgrade Dialog box appears showing Step 5 of the wizard (Figure 4-15).

*Figure 4-15   Inserting the STM-N cards into the protect slots*
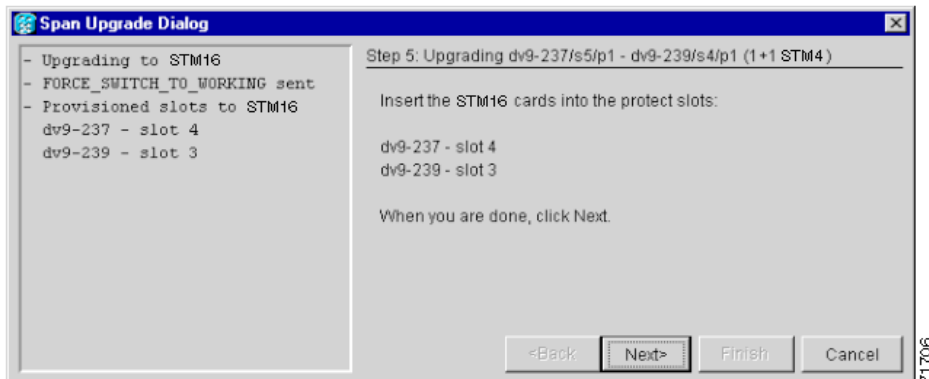


Step 9    Install the higher-rate STM-N cards into the protect slots.

Step 10    Install the fiber and click **Next**. The Span Upgrade Dialog box appears showing Step 6 of the wizard (Figure 4-16 on page 4-29).

*Figure 4-16    Sending a force switch command*
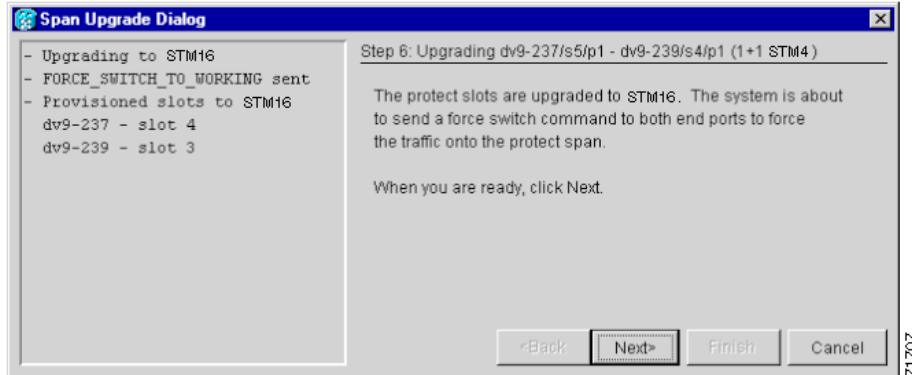


**Step 11**    Click **Next** to send a force switch command, forcing traffic to the protect lines. The Span Upgrade Dialog box appears showing Step 7 of the wizard (Figure 4-17).

*Figure 4-17    Waiting for the force switch command to take effect*
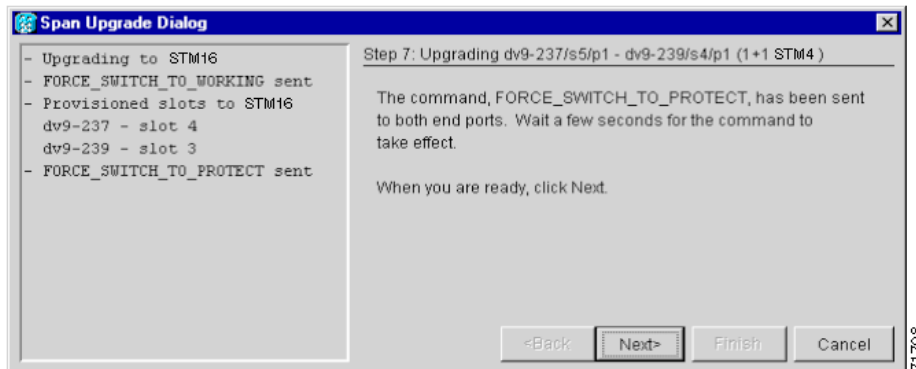


**Step 12**    Wait 5 to 10 seconds for the command to take effect and click **Next**. An error dialog box appears if more time is needed. The Span Upgrade Dialog box appears showing Step 8 of the wizard (Figure 4-18).

*Figure 4-18    Removing the STM-N cards from the working slots*
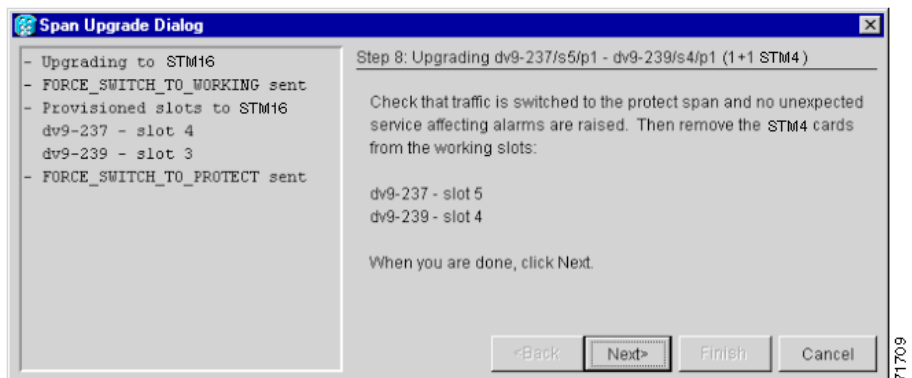


**Step 13**    Remove the fiber and ensure that traffic is still running.

**Step 14** Remove the lower-rate STM-N cards from the working slots and click **Next>**. The Span Upgrade Dialog box appears showing Step 9 of the wizard (Figure 4-19).

*Figure 4-19   Inserting the STM-N cards into the working slots*
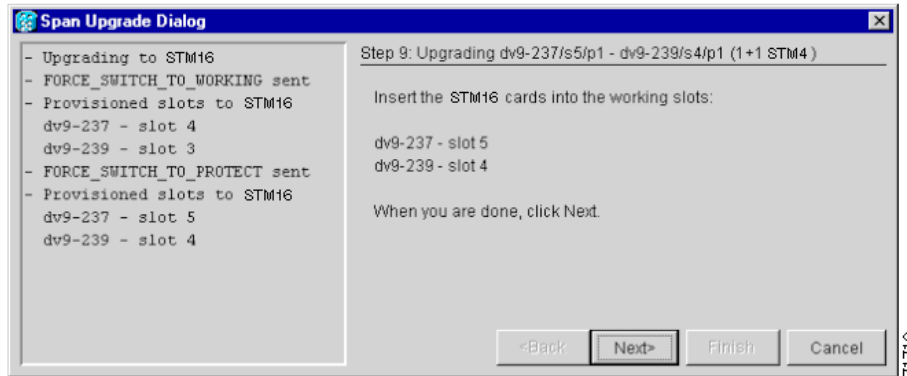


**Step 15** Insert the higher-rate STM-N cards in the working slots.

**Step 16** Install the fiber and click **Next**. The Span Upgrade Dialog box appears showing Step 10 of the wizard (Figure 4-20).

*Figure 4-20   Sending a clear command*
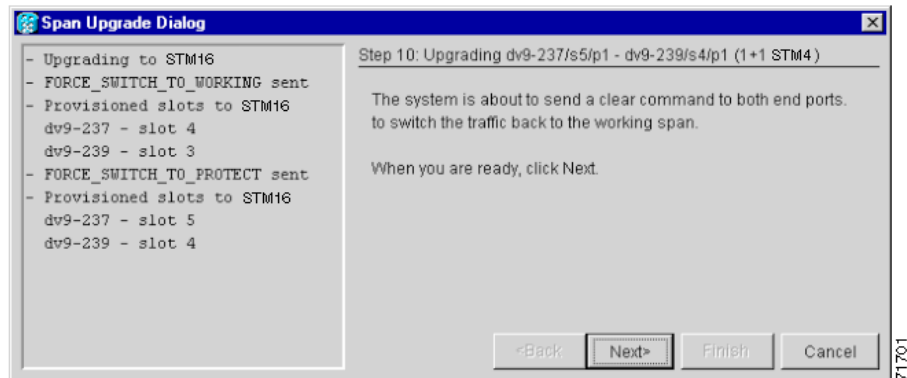


**Step 17** Click **Next** to send a clear command. The Span Upgrade Dialog box appears showing Step 11 of the wizard (Figure 4-21 on page 4-31).

*Figure 4-21   Completing the Span Upgrade wizard*
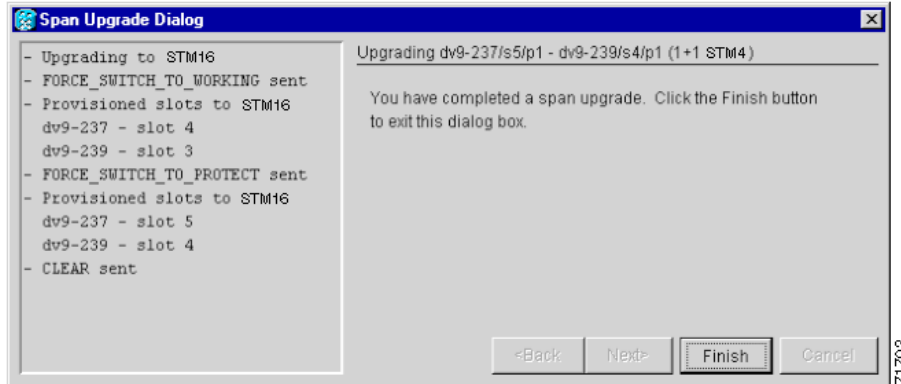


**Step 18**   Click **Finish**.

# 4.7.2 Manual Span Upgrades

The manual upgrade procedures require at least two technicians (one at each end of the span). The technicians must be able to communicate with each other during the upgrade. The upgrade procedures do not affect service. They cause no more than three switches with switch times of less than 50 ms.

During upgrade, some minor alarms and conditions occur and clear automatically. However, no service-affecting alarms (SA, Major, or Critical) should be expected. If any service-affecting alarms occur, Cisco recommends backing out of the procedure. Choose from four manual span upgrade options.

- Manually Upgrade a Span on a Two-Fiber MS-SPRing, page 4-31
- Manually Upgrade a Span on a Four-Fiber MS-SPRing, page 4-32
- Manually Upgrade a Span on a 1+1 Group, page 4-33
- Manually Upgrade a Span on a 1+1 Group, page 4-33

## Procedure: Manually Upgrade a Span on a Two-Fiber MS-SPRing

| | |
|---|---|
| **Purpose** | This procedure manually upgrades a span on a two-fiber MS-SPRing. |
| **Tools/Equipment** | STM cards that support the new line rate |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Note**   All lines connecting the nodes in an MS-SPRing must be upgraded before the added bandwidth is available.

**Step 1**   In the node view of the CTC software, click the **Conditions** tab.

**Step 2**   Click **Retrieve Conditions**. Ensure no abnormal conditions are present on the span to be upgraded.

**Step 3**   Click the **Alarms** tab.

**Step 4**      Ensure no alarms are present on the span to be upgraded.

**Step 5**      Apply a forced switch on the span that you will upgrade.

    **a.** In node view, click the **Maintenance > MS-SPRing** tabs.

    **b.** Click either the West Switch or the East Switch field and choose **FORCE RING** from the pull-down menu.

    **c.** Click **Apply**.

**Step 6**      Remove the fiber from both ends and ensure that traffic is still running.

**Step 7**      Pull the STM-N cards from both nodes.

**Step 8**      In node view of the CTC software, right-click each STM-N card slot and choose **Change Card** from the shortcut menu.

**Step 9**      In the Change Card dialog box, select the STM-N card type from the list box.

**Step 10**     Click **OK**.

**Step 11**     Insert the STM-N cards in both nodes.

**Step 12**     Install the fiber in both nodes.

**Step 13**     Wait for the IMPROPRMVL alarm to clear and for the cards to become active.

**Step 14**     If cards on each side of the line have been successfully upgraded, remove the forced switch.

    **a.** In the node view, click the **Maintenance > MS-SPRing** tabs.

    **b.** Click either the West Switch or the East Switch field and choose **CLEAR** from the pull-down menu.

    **c.** Click **Apply**.

**Step 15**     Repeat Steps 1 to 14 for each span in the MS-SPRing.

## Procedure: Manually Upgrade a Span on a Four-Fiber MS-SPRing

| | |
|---|---|
| **Purpose** | Manually upgrading a span on a four-fiber MS-SPRing |
| **Tools/Equipment** | STM cards that support the new line rate |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

When upgrading a four-fiber MS-SPRing, you can upgrade both working and protect lines with a single force switch.

![Note icon]

**Note**    All lines in an MS-SPRing must be upgraded before added bandwidth will be available.

**Step 1**      In the node view of the CTC software, click the **Conditions** tab.

**Step 2**      Click **Retrieve Conditions**. Ensure no abnormal conditions are present on the span to be upgraded.

**Step 3**      Click the **Alarms** tab.

**Step 4**      Ensure no alarms are present on the span to be upgraded.

**Step 5**    Apply a forced switch on the ports that you will upgrade.

    **a.**    In the node view, click the **Maintenance > MS-SPRing** tabs.

    **b.**    Click either the West Switch or the East Switch column and choose **FORCE RING** from the pull-down menu.

    **c.**    Click **Apply**.

**Step 6**    Remove the fiber from both ends of both spans and ensure that traffic is still running.

**Step 7**    Pull the four STM-N cards (two from each node).

**Step 8**    In the node view, right-click each STM-N card slot and choose **Change Card** from the shortcut menu.

**Step 9**    In the Change Card dialog box, select the STM-N card type from the list box.

**Step 10**    Click **OK**.

**Step 11**    Insert the four STM-N cards in both nodes (two in each).

**Step 12**    Install the fiber at both ends.

**Step 13**    Wait for the IMPROPRMVL alarm to clear and for the cards to become active.

**Step 14**    If cards on each side of the line have been successfully upgraded, remove the forced ring switch.

    **a.**    In the node view, click the **Maintenance > MS-SPRing** tabs.

    **b.**    Click either the West Switch or the East Switch field and choose **CLEAR** from the menu.

    **c.**    Click **Apply**.

**Step 15**    Repeat Steps 1 to 14 for each span in the MS-SPRing.

## Procedure: Manually Upgrade a Span on a 1+1 Group

When upgrading a 1+1 group, upgrade the working and protect span regardless of which line is active. Both lines in a 1+1 group must be upgraded before added bandwidth will be available.

| | |
|---|---|
| **Purpose** | Upgrading a span on a 1+1 group manually |
| **Tools/Equipment** | STM cards that support the new line speed |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**    In the node view of the CTC software, click the **Conditions** tab.

**Step 2**    Click **Retrieve Conditions**. Ensure no abnormal conditions are present on the span to be upgraded.

**Step 3**    Click the **Alarms** tab.

**Step 4**    Ensure no alarms are present on the span to be upgraded.

**Step 5**    Apply a forced switch away from the span that you will upgrade.

    **a.**    In the node view, click the **Maintenance > Protection** tabs.

    **b.**    In the Protection Groups list box, choose the 1+1 protection group.

    **c.**    Click the working/active card of the selected groups.

    **d.**    Click **Switch** and **OK**.

**Step 6**    Remove the fiber from both nodes and ensure that traffic is still running.

**Step 7**    Pull the STM-N cards from both nodes.

**Step 8**    In the node view, right-click each STM-N card slot and choose **Change Card** from the shortcut menu.

**Step 9**    In the Change Card dialog box, choose the STM-N card type from the list box

**Step 10**    Click **OK**.

**Step 11**    Insert the STM-N cards in both nodes.

**Step 12**    Install the fibers at both ends.

**Step 13**    Wait for the IMPROPRMVL alarm to clear and for the card to become standby.

**Step 14**    If cards on each side of the span have been successfully upgraded, remove the forced switch..

    **a.**  In the node view, click the **Maintenance > Protection** tabs.

    **b.**  In the Protection Groups list box, choose the 1+1 protection group.

    **c.**  Click the protect/standby card of the selected groups.

    **d.**  Click **Clear** and **OK**.

    **Note**    You cannot downgrade if circuits exist on the STM-Ns that would be removed (i.e., the higher STM-Ns).

**Step 15**    Repeat Steps 1 to 14 for any other lines in the 1+1 group.

# 4.8  Inspect and Clean Fiber Connectors

| | |
|---|---|
| **Purpose** | This procedure is used to clean and inspect fiber connectors. |
| **Tools/Equipment** | • Inspection videoscope |
| | • Compressed air/duster |
| | • "Type A" Fiber Optic Connector Cleaner (Cletop reel) |
| | • Isopropyl alcohol 70% or higher |
| | • Optical swab |
| | • Optical receiver cleaning stick |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Warning**    **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

**Caution**    Be sure traffic is switched away from a fiber span before you remove fiber for cleaning.

⚠

**Caution**    Before cleaning the optical connectors in an optical card, remove the card from the subrack and place it on a suitable anti-static mat.

⚠

**Caution**    Do not reuse the optical swabs. Keep unused swabs off of work surfaces.

**Step 1**    Using an inspection videos cope, inspect each fiber connector for dirt, cracks, or scratches. Refer to the "Inspect a Fiber Connector" task on page 4-35 for information if there is not a site-standard practice for inspection.

**Step 2**    Replace any damaged fiber connectors.

✎

**Note**    Replace all dust caps whenever the equipment will be unused for 30 minutes or more.

**Step 3**    Complete the "Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes" task on page 4-36 or the "Clean and Scope Fiber Connectors, Using Cletop" Procedure on page 4-36 as necessary and according to site practice.

**Step 4**    Complete the "Clean a Fiber Adapter" task on page 4-37 as necessary.

**Step 5**    Complete the "Clean a Feedthrough Connector" task on page 4-37 as necessary.

**Step 6**    Complete the "Inspect a Fiber Connector" task on page 4-35 to confirm fiber cleanness as necessary.

## Procedure: Inspect a Fiber Connector

| | |
|---|---|
| **Purpose** | Inspecting optical connectors |
| **Tools/Equipment** | • Video fiber connector inspection instrument |
| | • Cletop cleaning cassette |
| | • Compressed air |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**    Check the optical connector for large scratches using a video fiber connector inspection instrument. If you find a scratch, replace the connector. A connector is replaced by splicing a new pigtail.

**Step 2**    Check the connector end surface under the videoscope. If dark spots are seen on the surface of the ends, they are caused by dirt or possible damage. Pay special attention to the core-surface.

**Step 3**    If you cannot eliminate the spots by cleaning, this indicates damage to the glass fiber. You must replace the connector.

## Procedure: Clean and Scope Fiber Connectors, Using Alcohol and Dry Wipes

| | |
|---|---|
| **Purpose** | This task is used to clean the fiber connectors and adapters with alcohol and dry wipes. |
| **Tools/Equipment** | • Fiber inspection videoscope |
| | • Compressed air/duster |
| | • Isopropyl alcohol (70% or higher) and optical swab, or |
| | • Premoistened alcohol wipe |
| | • Optical receiver cleaning stick |
| **Prerequisite Procedures** | — |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |

⚠ **Warning** **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

**Step 1** Remove the dust cap from the fiber connector.

**Step 2** Wipe the connector tip with a premoistened alcohol wipe or swap and alcohol.

**Step 3** Blow the connector tip dry using filtered air.

**Step 4** Use an inspection videos cope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Step 1–3. Use the Inspect a Fiber Connector procedure if there is not a site standard practice for inspection.

**Step 5** Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

✎ **Note** If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry lint free wipe and the inside of the dust cap using a Cletop stick swab (14100400).

## Procedure: Clean and Scope Fiber Connectors, Using Cletop

| | |
|---|---|
| **Purpose** | This task is used to clean the fiber connectors with Cletop. |
| **Tools/Equipment** | • "Type A" Fiber Optic Connector Cleaner (Cletop reel) |
| | • Fiber inspection videoscope |
| **Prerequisite Procedures** | — |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |

**Step 1** Remove the dust cap from the fiber connector.

**Step 2** Press the lever down on the Cletop to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

**Step 3** Insert the connector into the Cletop cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

**Step 4** Use an inspection videos cope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Step 1–3. Use the Inspect a Fiber Connector procedure if there is not a site standard practice for inspection.

**Step 5** Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

> ✎
> **Note** If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry lint free wipe and the inside of the dust cap using a Cletop stick swab (14100400).

## Procedure: Clean a Fiber Adapter

| | |
|---|---|
| **Purpose** | This task is used to clean fiber adapters. |
| **Tools/Equipment** | Cletop stick swab |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1** Remove the dust plug from the fiber adapter.

**Step 2** Insert a Cletop stick swab (14100400) into the adapter opening and rotate the swab.

**Step 3** Place dust plugs on the fiber adapters when not in use.

## Procedure: Clean a Feedthrough Connector

| | |
|---|---|
| **Purpose** | Cleaning a feedthrough connector |
| **Tools/Equipment** | Compressed air |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1** Inspect the feedthrough connector with the naked eye.

**Step 2** Remove any dust with compressed air.

**Step 3** Inspect again. If there is resistant dirt or grease, or if there are mechanical defects, replace the connector.

# 4.9  Powering Down a Node

✎
**Note**    Always use the ESD wristband when working with the Cisco ONS 15454 SDH. Plug the wristband into the ESD jack located on the right outside of the shelf assembly. The front door is grounded to prevent electrical shock.

✎
**Note**    The procedure minimizes traffic outages when nodes are powered down, but traffic will be lost if you delete and recreate circuits that passed through a working node.

## Procedure: Power Down a Node

| | |
|---|---|
| **Purpose** | Powering down a node |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**    Identify the node to be powered down. If no cards are installed, go to Step 14. If one or two TCC-I cards are installed, log into the node.

**Step 2**    From the CTC software network view, log into the node and verify that the node is not connected to a working network.

To determine whether the node is part of a working network, click Go to the Network View in the CTC node view, and determine whether the node is connected to other nodes on the map by spans.

To determine what kind of configuration the node is included in (if it is still part of a working network), log into the node if you have not done so already and click the Provisioning > MS-SPRing tab in the CTC node (default login) view. If a ring is present on the tab, the node is part of a two- or four-fiber MS-SPRing. If it is not present, but still shown on the network view map, it is an SNMP or linear ADM node.

- If the node is part of a working network, log out of the node and refer to the *Cisco ONS 15454 SDH Installation and Operations Guide* for procedures to remove nodes. Then continue with Step 3.

- If the node is not connected to a working network and the current configurations are no longer required, go to Step 3.

    ✎
    **Note**    Current configurations will be saved if Steps 3 to 10 are skipped.

**Step 3**    From the node view, click the **Circuits** tab and verify that no circuits are displayed. If circuits are displayed, delete all the circuits that originate or terminate in the node.

   **a.**  Click the circuits that need to be deleted and click **Delete**.

   **b.**  Click **Yes** in the Delete Circuits dialog box.

If no circuits are displayed, skip to Step 4.

**Step 4**    From the node view, choose the **Provisioning > Protection** tabs and delete all protection groups.

**Step 5**   From the node view, choose the **Provisioning > SDH DCC** tabs and delete all SDCC terminations.

**Step 6**   Click **Yes** in the Delete SDCC Terminations dialog box and **Yes** in the "Are you sure?" confirmation dialog box.

**Step 7**   For an installed line card, from the card view, click the **Provisioning > Line** tabs and place all ports in the OOS state by clicking the row for each port under the State column and choosing **OOS** from the list box.

**Step 8**   Click **Apply** and **Yes** in the Confirmation Dialog.

**Step 9**   Remove all fiber connections to the cards.

**Step 10**   Right-click the installed line card in CTC and click **Delete** from the shortcut menu.

**Step 11**   Click **Yes** in the "Are you sure?" confirmation dialog box.

**Step 12**   After you have deleted the line card, open the card ejector handles for each card and pull it from the node. Repeat Steps 7 to 12 for each installed line card.

**Step 13**   Turn off the power of the power supply that feeds the node.

**Step 14**   Disconnect the power cables from the external source.

**Step 15**   Disconnect the power cables from the MIC-A/P and MIC-C/T/P cards.

**Step 16**   Remove all the remaining common cards and FMEC cards from the node.

**Step 17**   Store all pulled cards and update inventory records according to local site practice.

# 4.10  Powering Up a Node

**Note**   Always use the ESD wristband when working with the Cisco ONS 15454 SDH. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf assembly. To access the ESD plug on the shelf assembly, open the front door of the Cisco ONS 15454 SDH. The front door is grounded to prevent electrical shock.

## Procedure: Power Up a Node

| | |
|---|---|
| **Purpose** | This procedure powers up a node. |
| **Tools/Equipment** | — |
| **Prerequisite Procedures** | — |
| **Onsite/Remote** | Onsite |

**Step 1**   Make sure that the fan trays are installed in the shelf. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 2**   Install the first TCC-I card in the shelf. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 3**   Install the MIC-A/P in Slot 23 and the MIC-C/T/P card in Slot 24 of the shelf. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide.*

**Step 4**   Connect the power cables to the power supply inputs of the MIC-A/P and the MIC-C/T/P.

**Step 5**  Connect the other ends of the power cables to the power distribution panel. Refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 6**  Turn on both power switches on the power distribution panel.

**Step 7**  Ensure that the fans are running.

**Step 8**  Wait until the first TCC-I card has finished its startup procedure. The startup procedure takes about three minutes and is finished when the IP address is to displayed on the LCD of the fan unit.

**Step 9**  Install the second TCC-I.

> ✎
>
> **Note**  When a second TCC-I card is inserted into the shelf, it will synchronize its software, its backup software, and its database with the active TCC-I. If its software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy from the active TCC-I. This copying will take about 15 to 20 minutes. If its backup software version does not match the version on the active TCC-I, the newly inserted TCC-I will copy the backup software from the active TCC-I. This copying, again, will take about 15 to 20 minutes. Copying the database from the active TCC-I will take about 3 minutes. So, depending on the software existing in the new TCC-I, booting it up will take between 3 and about 40 minutes.

**Step 10**  Install the first and the second XC10G cards. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 11**  Install the optical line cards required for the configuration to be set up.For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 12**  Install the electrical line cards required for the configuration to be set up. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 13**  Install the FMECs required for the configuration to be set up. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 14**  Check with the fiber video videos cope and, if necessary, clean each fiber connector using the procedures in Inspect and Clean Fiber Connectors, page 4-34.

**Step 15**  Install all fiber connections to the cards as required for the configuration to be set up. For instructions, refer to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

**Step 16**  Configure the node according to the *Cisco ONS 15454 SDH Installation and Operations Guide*.

# Numerics

### 1:1 protection

An electrical card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot (DS-1 and DS-3 speeds). If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts to the working card.

### 1+1 protection

An optical (OC-N) card protection scheme that pairs a single working port/card with a single dedicated protect port/card. All OC-N cards can use this protection type (OC-3, OC-12, OC-48, and OC-192 speeds).

### 1:N protection

An electrical card protection scheme that allows a single protect card to provide protection for several working cards (DS-1 and DS-3 speeds). If a working card fails, the traffic from the working card switches to the protect card.When the failure on the working card is resolved, traffic reverts to the working card.

### 10BaseT

Standard 10 Mbps local area network over unshielded twisted pair copper wire.

### 100BaseT

Standard 100 Mbps local ethernet network.

### 100BaseTX

Specification of 100BaseT that supports full duplex operation.

# A

### Access drop

Points where network devices can access the network.

### ACO

Alarm cutoff.

### Active card

A card that is working or carrying traffic. A card provisioned as working can be an active card or, after a protection switch, a protect card can be an active card.

**ACT/STBY**

Active/Standby.

**Address mask**

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the portion that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

**ADM**

(Add/drop multiplexers). Linear ADMs allow signals to be added to a SONET span or dropped from a SONET span. An ADM has three or more nodes.

**Agent**

1. 1. Generally, software that processes queries and returns replies on behalf of an application.

2. 2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

**AIC**

Alarm Interface Controller.

**AID**

(Access Identifier). An access code used in TL1 messaging that identifies and addresses specific objects within the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and others. See also *TID*.

**AIP**

Alarm Interface Panel.

**AIS**

Alarm Indication Signal.

**AIS-L**

Line Alarm Indication Signal.

**AMI**

(Alternate Mark Inversion). Line-code format used on T1 circuits that transmits ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

**ANSI**

American National Standards Institute.

**APS**

(Automatic Protection Switching). SONET switching mechanism that routes traffic from working lines to protect lines if a line card failure or fiber cut occurs.

**ARP**

Address Resolution Protocol.

**APSB**

Alarm Protection Switching Byte.

**ATAG**

(Autonomous Message Tag). ATAG is used for TL1 message sequencing. See also *CTAG*.

**ATM**

Asynchronous Transfer Mode.

**AWG**

American Wire Gauge

# B

**B8ZS**

(Binary 8-zero Substitution). A line-code type, used on T1 circuits, that substitutes a special code whenever 8 consecutive zeros are sent over the link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream. Sometimes called bipolar 8-zero substitution.

**Backbone**

The part of the network that carries the heaviest traffic or joins LANs together.

**BER**

(Bit Error Rate). Ratio of received bits that contain errors.

**BIC**

Backplane Interface Connector.

**BIP**

Bit Interleaved Parity.

**Bit rate**

Speed at which bits are transmitted, usually expressed in bits per second.

**BITS**

(Building Integrated Timing Supply). A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

**BLSR**

(Bidirectional Line Switched Ring). SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber. See also *UPSR*.

**Blue band**

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 SDH operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

**BNC**

Bayonet Neill-Concelman (coaxial cable bayonet-locking connector).

**BPDU**

Bridge Protocol Data Unit.

**Bridge**

Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame. See also *MAC address*.

**Broadcast**

Data packet that will be sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

**Broadcast address**

Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones. See also *MAC address.*

**Broadcast storm**

Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

**Bus**

Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

# C

**C2 byte**

The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. See also *SONET*.

**CAT 5**

Category 5 (cabling).

**CCITT**

Comité Consultatif International Télégraphique et Téléphoniques. (Formerly ITU.)

**CEO**

Central Office Environment.

**CEV**

Controlled Environment Vaults.

**CLEI**

Common Language Equipment Identifier code.

**CLNP**

Correctionless Network Protocol.

**cm**

Centimeter.

**CMIP**

Common Management Information Protocol.

**COE**

Central Office Environment.

**Collision**

In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

**Concatenation**

A mechanism for allocating contiguous bandwidth for payload transport. Through the use of Concatenation Pointers, multiple OC-1s can be linked together to provide contiguous bandwidth through the network, from end to end.

**CORBA**

Common Object Request Broker Architecture.

**CPE**

Customer Premise Environments.

**Crosspoint**

A set of physical or logical contacts that operate together to extend the speech and signal channels in a switching network.

**CTAG**

(Correlation Tag). A unique identifier given to each input command by the TL1 operator. When the ONS 15454 system responds to a specific command, it includes the command's CTAG in the reply. This eliminates discrepancies about which response corresponds to which command. See also *ATAG*.

**CTC**

(Cisco Transport Controller). A Java-based graphical user interface (GUI) that allows operations, administration, maintenance, and provisioning (OAM&P) of the ONS 15454 using an Internet browser.

**CTM**

(Cisco Transport Manager). A Java-based network management tool used to support large networks of Cisco 15000-class D

**DCC**

(Data Communications Channel). Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCC can be located in SDCC or LDCC. See also *LDCC* and *SDCC*.

**DCN**

Data Communications Network.

**DCS**

Distributed Communications System.

**Default router**

If the ONS 15454 must communicate with a device on a network to which the ONS 15454 is not connected, packets are sent to this router to be distributed.

**Demultiplex**

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. Compare *Multiplexing*.

**Destination**

The endpoint where traffic exits an ONS 15454 network. Endpoints can be paths (STS or STS/VT for optical card endpoints), ports (for electrical circuits, such as DS1, VT, DS3, STS), or cards (for circuits on DS1 and Ethernet cards). See also STS, and *VT*.

**DRAM**

Dynamic Random-Access Memory.

**Drop**

See *Destination*.

**DS-1**

Digital Signal Level One.

**DS1-14**

Digital Signal Level One (14 ports).

**DS1N-14**

Digital Signal Level One (N-14 ports).

**DS-3**

Digital Signal Level Three.

**DS3-12**

Digital Signal Level Three (12 ports).

**DS3N-12**

Digital Signal Level Three (N-12 ports).

**DS3XM-6**

Digital Service, level 3 Trans-Multiplexer 6 ports.

**DSX**

(Digital Signal Cross-Connect Frame). A manual bay or panel where different electrical signals are wired. A DSX permits cross-connections by patch cords and plugs.

**DWDM**

(Dense Wave Division Multiplexing). A technology that increases the information carrying capacity of existing fiber optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.

# E

**EDFA**

(Erbium Doped Fiber Amplifier). A type of fiber optical amplifier that transmits a light signal through a section of erbium-doped fiber and amplifies the signal with a laser pump diode. EDFA is used in transmitter booster amplifiers, in-line repeating amplifiers, and in receiver preamplifiers.

**EFCA**

Electrical Facility Connection Assembly.

**EFT**

Electrical Fast Transient/Burst.

**EIA**

(Electrical Interface Assemblies). Provides backplane connection points for the DS-1, DS-3, and EC-1 cards.

**ELR**

Extended Long Reach.

**EMC**

Electromagnetic compatibility.

**EMI**

(Electromagnetic Interference). Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

**EML**

Element Manager Layer.

**EMS**

Element Management System.

**Envelope**

The part of messaging that varies in composition from one transmittal step to another. It identifies the message originator and potential recipients, documents its past, directs its subsequent movement by the Message Transfer System (MTS), and characterizes its content.

**EOW**

(Engineered Orderwire). A permanently connected voice circuit between selected stations for technical control purposes.

**ERDI**

Enhanced Remote Defect Indicator.

**ES**

Errored Seconds.

**ESD**

Electrostatic Discharge.

**ESF**

Extended Super Frame.

**Ethernet switch**

A type of Ethernet LAN device that increases aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously shared LAN segments into multiple networks with fewer stations per network.

**ETSI**

European Telecommunications Standards Institute.

**Extended SNCP**

(Extended Subnetwork Connection Protection). Extended SNCP extends the protection scheme of a subnetwork connection protection ring (SNCP) beyond the basic ring configuration to the meshed architecture of several interconnecting rings. See *SNCP*.

**External timing reference**

A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

## F

**Falling threshold**

A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

**FC**

Failure count.

**FDDI**

(Fiber Distributed Data Interface). LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

**FE**

Frame Bit Errors.

**FG1**

Frame Ground #1 (pins are labeled "FG1," "FG2," etc.)

**FMEC**

Front Mount Electrical Connection.

**Frame**

Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

**FSB**

Field Service Bulletin.

## G

**Gateway**

An electronic repeater device that intercepts and steers electrical signals from one network to another.

**GBIC**

(Gigabit Interface Converter). A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

**Gbps**

Gigabits per second.

**GBps**

Gigabytes per second.

**GR-153-CORE**

General Requirements #253 Council of Registrars.

**GR-1089**

General Requirements #1089.

**GUI**

Graphical User Interface.

# H

**Hard reset**

The physical removal and insertion of a TCC+ card, also known as reseating a card or performing a card pull.

**HDLC**

(High-Level Data Link Control). Bit-oriented, synchronous, data-link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

**Host number**

Part of IP address used to address an individual host within the network or subnetwork.

**Hot swap**

The process of replacing a failed component while the rest of the system continues to function normally.

# I

**IEC**
1.  1. InterExchange Carrier.
2.  2. International Electrotechnical Commission.

**IEEE**

Institute of Electrical and Electronics Engineers.

**IETF**

Internet Engineering Task Force.

**Input alarms**

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

**I/O**

Input/Output.

**IP**

(Internet Protocol). Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

**IPPM**

Intermediate-Path Performance Monitoring.

**IP address**

32-bit address assigned to host using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.

**ITU-T**

International Telecommunication Union - Telecommunication Standards Sector.

# J

**JRE**

Java Runtime Environment.

# K

**K bytes**

Automatic protection-switching bytes located in the SONET line overhead and monitored by equipment for an indication to switch to protection.

# L

**LAN**

(Local Area Network). High-speed, low error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

**LCD**

(Liquid Crystal Display). An alphanumeric display using liquid crystal sealed between two pieces of glass. LCDs conserve electricity.

**LDCC**

Line Data Communication Channel.

**Line layer**

Refers to the segment between two SONET devices in the circuit. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization. Sometimes called a maintenance span.

**Line terminating equipment (LTE)**

Refers to line cards which terminate the line signal in the ONS 15454.

**Line timing mode**

A node that derives its clock from the SONET lines.

**Link budget**

The difference between the output power and receiver power of an optical signal expressed in dB. Link refers to an optical connection and all of its component parts (optical transmitters, repeaters, receivers, and cables).

**Link integrity**

The network communications channel has link integrity if it is intact.

**LOF**

Loss of Frame.

**Loopback test**

Test that sends signals then directs them back toward their source from some point along the communications path. Loopback tests are often used to test network interface usability.

**LOP**

Loss of Pointer.

**LOS**

Loss of Signal.

**LOW**

(Local Orderwire). A communications circuit between a technical control center and selected terminal or repeater locations.

**LTE**

Line Terminating Equipment.

**LVDS**

Low-Voltage Differential Signal.

# M

**MAC**

Media Access Control.

**MAC address**

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as the hardware address, MAC-layer address, and physical address.

**Maintenance user**

A security level that limits user access to maintenance options only. See also *Superuser*, *Provisioning User*, and *Retrieve User.*

**Managed device**

A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers.

**Managed object**

In network management, a network device that can be managed by a network management protocol. Sometimes called an MIB object.

**Mapping**

A logical association between one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

**Mbps**

Megabits per second.

**MBps**

Megabytes per second.

**MHz**

Megahertz.

**MIB**

(Management Information Base). Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MIME**

Multipurpose Internet Mail Extensions.

**MS**

Multiplex Section.

**MS-FERF**

Multiplex Section Far-end Receive Failure.

**MSP**

Multiplex Section Protection.

**MS-SPRing**

(Multiplex Section Shared Protection Ring.) SDH ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically rerouted onto the protection fiber.

**Multicast**

Single packets copied by the network and sent to a specific subset of network addresses.

**Multiplex payload**

Generates section and line overhead, and converts electrical/optical signals when the electrical/optical card is transmitting.

**Multiplexing**

Scheme that allows multiple signals to be transmitted simultaneously across a single physical channel. Compare *Demultiplex*.

**Mux/Demux**

Multiplexer/Demultiplexer.

**Muxed**

Multiplexed. See *Multiplexing*.

# N

**NE**

(Network Element). In an Operations Support System, a single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

**NEBS**

Network Equipment-Building Systems.

**NEL**

Network Element Layer.

**Network number**

Part of an IP address that specifies the network where the host belongs.

**NML**

Network Management Layer.

**NMS**

(Network Management System). System that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.

**Node**

Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network. Node is sometimes used generically to refer to any entity that can access a network. In this manual the term "node" usually refers to an ONS 15454.

# O

**OAM&P**

(Operations, Administration, Maintenance, and Provisioning). Provides the facilities and personnel required to manage a network.

**OC**

Optical carrier.

**OOS AS**

Out of Service Assigned.

**Optical amplifier**

A device that amplifies an optical signal without converting the signal from optical to electrical and back again to optical energy.

**Optical receiver**

An opto-electric circuit that detects incoming lightwave signals and converts them to the appropriate signal for processing by the receiving device.

**Orderwire**

Equipment that establishes voice contact between a central office and carrier repeater locations. See *Local orderwire*.

**OSI**

Open Systems Interconnection.

**OSPF**

Open Shortest Path First.

**OSS**

Operations Support System.

**OSS/NMS**

Operations Support System/Network Management System.

**Output contacts (controls)**

Triggers that drive visual or audible devices such as bells and lights. Output contacts can control other devices such as generators, heaters, and fans.

# P

**Passive devices**

Components that do not require external power to manipulate or react to electronic output. Passive devices include capacitors, resisters, and coils.

**Path Layer**

The segment between the originating equipment and the terminating equipment. This path segment may encompass several consecutive line segments or segments between two SONET devices.

**Payload**

Portion of a cell, frame, or packet that contains upper-layer information (data).

**PCM**

Pulse Code Modulation.

**PCMCIA**

Personal Computer Memory Card International Association.

**PCN**

Product Change Notice(s).

**PDI-P**

STS Payload Defect Indication - Path.

**Ping**

(Packet internet grouper). ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

**Pointer justification**

In SONET, the mechanism used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks.

**POP**

Point of Presence.

**PM**

Performance Monitoring.

**PPMN**

(Path-Protected Mesh Network). PPMN extends the protection scheme of a unidirectional path switched ring (UPSR) beyond the basic ring configuration to the meshed architecture of several interconnecting rings.

**Priority queuing**

Routing feature that divides data packets into two queues: one low-priority and one high-priority.

**Protect card**

A card in a protection pair or scheme that is provisioned as a protect card to the working card. If the working card fails, the protect card becomes active. See also *working card*.

**Provisioning user**

A security level that allows the user to access only provisioning and maintenance options in CTC. See also *Superuser*, *Maintenance user,* and *Retrieve user.*

**PSC**

Protection-Switching Count.

**PSD**

Protection-Switching Duration.

**PTE**

Path-Terminating Equipment.

# Q

**Queue**

In routing, a backlog of packets waiting to be forwarded over a router interface.

# R

**RAM**

Random Access Memory.

**RDI-L**

Remote Defect Indication - Line.

**Red band**

DWDM wavelengths are broken into two distinct bands: red and blue. The red band is the higher frequency band. The red band DWDM cards for the ONS 15454 SDH operate on wavelengths between 1547.72nm and 1560.61nm.

**RES**

Reserved.

**Retrieve user**

A security level that allows the user to retrieve and view CTC information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user.*

**Revertive switching**

A process that sends electrical interfaces (traffic) back to the original working card after the card comes back online.

**Rising threshold**

The number of occurrences (collisions) that must be exceeded to trigger an event.

**RJ-45**

Registered Jack #45 (8-pin).

**RMA**

Return Materials Authorization.

**RMON**

(Remote Network Monitoring). Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

**RS-232**

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication).

**Rx**

Receive.

# S

**SCI**

Serial Communication Interface.

**SCL**

System Communications Link.

**SDCC**

Section Data Communication Channel.

**SDH**

(Synchronous Digital Hierarchy). European standard that defines a set of rate and format standards that are transmitted using optical signals over fiber. SDH is similar to SONET, with a basic SDH rate of 155.52 Mbps. Compare *SONET*.

**SEF**

Severely Errored Frame.

**SELV**

Safety Extra-Low Voltage.

**SES**

Severely Errored Seconds.

**SF**

Super Frame.

**SML**

Service Management Layer.

**SMF**

Single Mode Fiber.

**SNCP**

(Subnetwork Connection Protection Ring). Path-switched SDH rings that employ redundant, fiber-optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over.

**SNMP**

(Simple Network Management Protocol). Network management protocol used almost exclusively in TCP/IP networks. SNMP monitors and controls network devices and manages configurations, statistics collection, performance, and security.

**SNTP**

(Simple Network Time Protocol). Using an SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

**Soft reset**

A soft reset reloads the operating system, application software, etc., and reboots the TCC+ card. It does not initialize the ONS 15454 ASIC hardware.

**SONET**

(Synchronous Optical Network). High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

**Source**

The endpoint where traffic enters an ONS 15454 network. Endpoints can be a path (STS or STS/VT for optical card endpoints), port (for electrical circuits, such as DS1, VT, DS3, STS), or card (for circuits on DS1 and Ethernet cards). See also *STS* and *VT*.

**Span**

An optical path between two nodes.

**Spanning tree**

A loop-free subset of a network topology. See also *STA* and *STP*.

**SPE**

(Synchronous Payload Envelope). A SONET term describing the envelope that carries the user data or payload.

**SSM**

(Synchronous Status Messaging). A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

**STA**

(Spanning-Tree Algorithm). An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP.*

**Standby card**

A card that is not active or carrying traffic. A standby card can be a protect card or, after a protection switch, a working card can be a standby card.

**Static route**

A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.

**STP**

1. 1. Shielded Twisted Pair.
2. 2. Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm to enable a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. See also *Spanning tree and STA.*

**STS**

(Synchronous Transport Signal, used generically when speaking of SONET signals.)

**STS-1**

(Synchronous Transport Signal Level 1). Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-*n*, where *n* is a multiple of 51.84 Mbps. See also *SONET.*

**Subnet mask**

32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address.*

**Subnetwork**

In IP networks, a network confined to a particular subnet address. Subnetworks are networks segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet.

**Subtending rings**

SONET rings that incorporate nodes that are also part of an adjacent SONET ring.

**Superuser**

A security level that can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A superuser is usually the network element administrator. See also *Retrieve user*, *Maintenance user*, and *Provisioning user*.

**SWS**

SONET WAN switch.

**SXC**

SONET Cross Connect ASIC.

# T

**T1**

T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network using AMI or B8ZS coding. See also *AMI*, *B8ZS*, and *DS-1*.

**TAC**

Technical Assistance Center.

**Tag**

Identification information, including a number plus other information.

**TBOS**

Telemetry Byte-Oriented Serial protocol.

**TCA**

Threshold Crossing Alert.

**TCC+**

Timing Communications and Control + Card

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**TDM**

(Time Division Multiplexing). Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

**TDS**

Time-Division Switching.

**Telcordia**

(Telcordia Technologies, Inc., formerly named Bellcore). Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

**TID**

(Target Identifier). Identifies the particular network element (in this case, the ONS 15454) where each TL1 command is directed. The TID is a unique name given to each system at installation. See also *AID*.

**TL1**

Transaction Language 1.

**TLS**

(Transparent LAN Service). Provides private network service across a SONET backbone.

**TMN**

Telecommunications Management Network.

**Transponder**

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength. See also *DWDM*.

**Trap**

Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold. See also *CTM*.

**Tributary**

The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low rate signals to form an aggregate higher rate level.

**Trunk**

Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

**TSA**

Time-Slot Assignment.

**TSI**

Time-Slot Interchange.

**Tunneling**

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

**Tx**

Transmit.

# U

**UAS**

Unavailable Seconds.

**UDP/IP**

User Datagram Protocol/Internet Protocol.

**UID**

User Identifier.

**Unicast**

The communication of a single source to a single destination.

**UPSR**

(Unidirectional Path Switched Ring). Path-switched SONET rings that employ redundant, fiber- optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over. See also *BLSR*.

**Upstream**

Set of frequencies used to send data from a subscriber to the head end.

**UTC**

Universal-Time Coordinated.

**UTP**

Unshielded Twisted Pair.

# V

**VDC**

Volts Direct Current.

**Virtual fiber**

A fiber that carries signals at different rates and uses the same fiber optic cable.

**Virtual ring**

Entity in a source-route bridging (SRB) network that logically connects two or more physical rings together either locally or remotely. The concept of virtual rings can be expanded across router boundaries.

**Virtual wires**

Virtual wires route external alarms to one or more alarm collection centers across the SONET transport network.

**VLAN**

(Virtual LAN). Group of devices located on a number of different LAN segments that are configured (using management software) to communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

**VPN**

(Virtual Private Network). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level. See also *Tunneling*.

**VT**

(Virtual Tributary). A structure designed for the transport and switching of sub-DS3 payloads. See also *Tributary*.

**VT1.5**

Virtual Tributary that equals 1.544 Mbps.

**VT layer**

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

# W

**W**

Watts.

**WAN**

Wide Area Network.

**Working card**

A card that is provisioned as an active, primary card. Traffic cards in a protection pair are provisioned as working or protect See also *Protect card*.

# X

**XC**

Cross Connect

**XCVT**

Cross Connect Virtual Tributary.

**X.25**

Protocol providing devices with direct connections to a packet-switched network.

# INDEX

## Numerics

1+1 optical card protection

> defined **GL-1**

1:1 electrical card protection

> defined **GL-1**

1:N electrical card protection

> defined **GL-1**

100BaseT

> defined **GL-1**

100BaseTX

> defined **GL-1**

10BaseT

> defined **GL-1**

## A

access drop   **GL-1**

Access Identifier

> defined   **GL-2**

ACO

> defined   **GL-1**

ACT/STBY

> defined   **GL-2**

active   **GL-1**

Address mask

> defined   **GL-2**

agent (software)

> defined   **GL-2**

AIC

> defined   **GL-2**

AIC card

> description   **3-17**

input/output (external) alarm contacts   **3-18**

> specifications   **3-21**

AID

> defined   **GL-2**

AID see Access Identifier

AIP   **GL-2**

> MFGMEM alarm   **1-79**

Air Filter

> Inspection   **4-2**

AIS   **1-14, GL-2**

AIS-L   **GL-2**

AIS-V alarm   **2-36**

Alarms

> see also Alarms by description

> alarms are also indexed individually by name

> CTC version for   **1-1**

> customer-defined (environmental) alarms   **3-18, 3-20, 3-21**

> listed alphabetically   **1-3**

> listed by alarm type   **1-5**

> listed by severity   **1-1**

> severities explained   **1-13**

> type definitions   **1-12**

Alarms by description

> administration unit AIS   **1-20**

> administration unit loss of pointer   **1-20**

> Alarms Suppressed by User Command   **1-18**

> Alarms Suppressed for Maintenance Command   **1-19**

> APS channel mismatch   **1-17**

> automatic laser off   **1-21**

> Automatic SNCP Switch Caused by AIS   **1-22**

> automatic SNCP switch caused by an LOP   **1-23**

> Automatic SNCP Switch Caused by Bit Error Rate Signal Degrade   **1-24**

---