CISCO SYSTEMS

Cisco ONS 15454 Troubleshooting and Maintenance Guide

Product and Documentation Release 3.2
Last Updated: December 27, 2004

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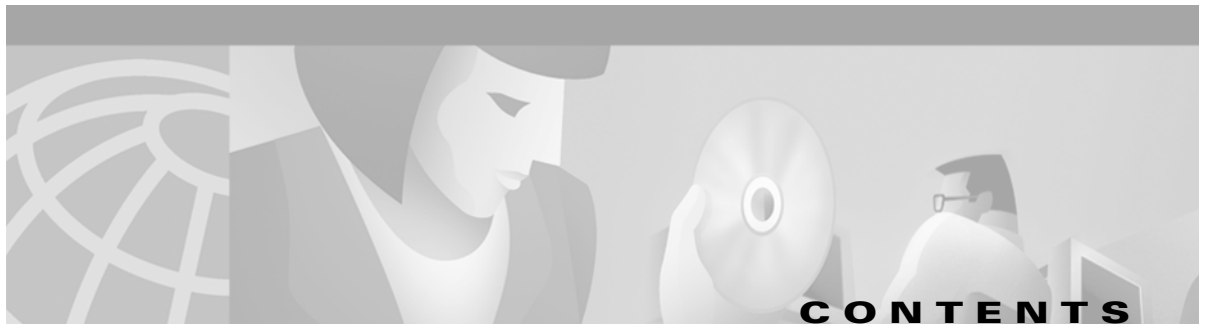
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, 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, GigaStack, 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. (0201R)

Cisco ONS 15454 Troubleshooting and Maintenance Guide, Release 3.2

ACRONYMS

GLOSSARY

INDEX

FIGURES

T A B L E S

Alarm Troubleshooting

General Troubleshooting

Maintenance

Card Reference

About This Manual

This section explains who should read the *Cisco ONS 15454 Troubleshooting and Maintenance Guide, R3.2 ,* 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 users who are responsible for troubleshooting and maintenance. General troubleshooting categories and a comprehensive list of ONS 15454 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 nodes should have the companion *Cisco ONS 15454 Installation and Operations Guide*. Users who require TL1 information should consult the *Cisco ONS 15454 TL1 Command Guide*.

Organization

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

Related Documentation

Cisco ONS 15454 Installation and Operations Guide, Release 3.2

Cisco ONS 15454 TL1 Command Guide, Release 3.2

Cisco ONS 15454 Product Overview, Release 3.2

Release Notes for the Cisco ONS 15454, Release 3.2

Cisco Warranty Services for ONG Products

Cisco ONS 15454 Quick Configuration Guide

Cisco ONS 15454 Quick Installation Guide

Cisco ONS 15454 Quick Reference for TL1 Commands, Release 3.2

Installing the Cisco ONS 15454 Conducted Emissions Kit (Required for EMEA compliance only)

Related products:

Cisco ONS 15216 EDFA2 Operations Guide

Installing the Cisco ONS 15216 100 Ghz DWDM Filters

Installing Cisco ONS 15216 OADMs

Cisco ONS 15216 Optical Performance Manager Operations Guide

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
Telcordia	Replaces all instances of Bellcore, the former name of Telcordia Technologies, Inc.
Cisco Transport Controller (CTC)	Replaces all instances of Cerent Management System (CMS)

Bold	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

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Release 3.2 of the *Cisco ONS 15454 Troubleshooting and Reference Guide*, *Cisco ONS 15454 Installation and Operations Guide*, and *Cisco ONS 15454 TL1 Command Reference Guid*e is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated as required. Therefore, it might be more current than printed documentation.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation, including the *Optical Networking Product* CD-ROM, from the Networking Products MarketPlace:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write 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 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 to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

Inquiries to Cisco TAC 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.

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

Cisco TAC Web Site

The Cisco TAC Web Site allows you 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 the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services 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 the following URL to register:

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following 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). In addition, please have available your service agreement number and your product serial number.

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each Cisco ONS 15454 alarm. Table 1-1 on page 1-1 gives an alphabetical list of alarms that appear on the ONS 15454. Table 1-2 on page 1-3 gives a list of alarms organized by alarm type. Both lists cross-reference the alarm entry, which gives the severity, description and troubleshooting procedure for each particular alarm.

The troubleshooting procedure for an alarm applies to both the CTC and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

The default standby severity for all ONS 15454 alarms is Minor, Non-service affecting, as defined in Telcordia GR-474. All severities listed in the alarm entry are the default for the active card, if applicable.

This chapter provides a comprehensive list of alarms (conditions with a severity of Minor, Major or Critical.) It also includes some conditions with severities of non-alarmed (NA) or not reported (NR), which are commonly encountered while troubleshooting major alarms. The default standby severity for conditions with a severity of NA, Non-service affecting (NSA) is NA, NSA. The default standby severity for conditions with a severity of NR, NSA is NR, NSA. For a comprehensive list of all conditions, see the *Cisco ONS 15454 TL1 Command Guide*.

1.1 Alarm Index

The alarm index list alarms by the name displayed on the CTC alarm pane in the conditions column.

Table 1-1   Alarm Index

AIS, page 1-9	FAILTOSWS, page 1-42	MEM-GONE, page 1-70
AIS-L, page 1-9	FAN, page 1-43	MEM-LOW, page 1-70
AIS-P, page 1-10	FE-AIS, page 1-43	MFGMEM, page 1-70
AIS-V, page 1-10	FE-DS1-MULTLOS, page 1-44	NOT-AUTHENTICATED, page 1-72
APSB, page 1-11	FE-DS1-SNGLLOS, page 1-44	PDI-P, page 1-72
APSCDFLTK, page 1-11	FE-DS3-SA, page 1-45	PEER-NORESPONSE, page 1-73
APSC-IMP, page 1-13	FE-EQPT-NSA, page 1-45	PLM-P, page 1-74
APSCINCON, page 1-13	FE-IDLE, page 1-46	PLM-V, page 1-75
APSCM, page 1-14	FE-LOCKOUT, page 1-46	PRC-DUPID, page 1-75
APSCNMIS, page 1-14	FE-LOF, page 1-46	RAI, page 1-76

Table 1-1   Alarm Index (continued)

APSMM, page 1-15	FE-LOS, page 1-47	RCVR-MISS, page 1-76
AUTOLSROFF, page 1-16	FEPRLF, page 1-47	RDI-P, page 1-77
AUTORESET, page 1-17	FORCED-REQ, page 1-48	RFI-L, page 1-77
AUTOSW-AIS, page 1-17	FRNGSYNC, page 1-48	RFI-P, page 1-77
AUTOSW-LOP (STSMON), page 1-17	FSTSYNC, page 1-48	RFI-V, page 1-78
AUTOSW-LOP (VT-MON), page 1-17	HITEMP, page 1-49	RING-MISMATCH, page 1-78
AUTOSW-PDI, page 1-18	HLDOVERSYNC, page 1-49	SD-L, page 1-79
AUTOSW-SDBER, page 1-18	IMPROPRMVL, page 1-50	SD-P, page 1-80
AUTOSW-SFBER, page 1-18	INCOMPATIBLE-SW, page 1-51	SF-L, page 1-81
AUTOSW-UNEQ (STSMON), page 1-18	INVMACADDR, page 1-52	SF-P, page 1-82
AUTOSW-UNEQ (VT-MON), page 1-18	LOCKOUT-REQ, page 1-52	SFTWDOWN, page 1-83
BKUPMEMP, page 1-18	LOF (BITS), page 1-53	SFTWDOWN-FAIL, page 1-83
BLSROSYNC, page 1-19	LOF (DS1), page 1-53	SQUELCH, page 1-85
CARLOSS (E-Series), page 1-21	LOF (DS3), page 1-54	SSM-FAIL, page 1-86
CARLOSS (EQPT), page 1-22	LOF (EC1-12), page 1-55	STU, page 1-86
CARLOSS (G1000-4), page 1-23	LOF (OC-N), page 1-55	SWMTXMOD, page 1-87
CONCAT, page 1-25	LOGBUFR90, page 1-56	SWTOPRI, page 1-88
CONTBUS-A, page 1-26	LOGBUFROVFL, page 1-57	SWTOSEC, page 1-88
CONTBUS-A-18, page 1-27	LOP-P, page 1-58	SWTOTHIRD, page 1-89
CONTBUS-B, page 1-28	LOP-V, page 1-59	SYNCPRI, page 1-89
CONTBUS-B-18, page 1-29	LOS (BITS), page 1-60	SYNCSEC, page 1-89
CTNEQPT-PBSTBY, page 1-29	LOS (DS-N), page 1-60	SYNCTHIRD, page 1-90
CTNEQPT-PBACT, page 1-31	LOS (EC1-12), page 1-61	SYSBOOT, page 1-91
DATAFLT, page 1-33	LOS (OC-N), page 1-62	TIM-P, page 1-91
DS3-MISM, page 1-33	LPBKDS1FEAC, page 1-63	TPTFAIL, page 1-91
EOC, page 1-33	LPBKDS3FEAC, page 1-63	TRMT, page 1-92
EQPT, page 1-35	LPBKFACILITY (DS-N or EC1-12), page 1-63	TRMT-MISS, page 1-93
EQPT-MISS, page 1-36	LPBKFACILITY (OC-N), page 1-64	UNEQ-P, page 1-93
E-W-MISMATCH, page 1-36	LPBKTERMINAL (DS-N, EC1-12), page 1-65	UNEQ-V, page 1-94
EXCCOL, page 1-38	LPBKTERMINAL (G1000-4), page 1-66	
EXERCISE-RING-FAIL, page 1-38	LPBKTERMINAL (OC-N), page 1-66	
EXERCISE-SPAN-FAIL, page 1-38	MAN-REQ, page 1-67	
EXT, page 1-39	MANRESET, page 1-67	
FAILTOSW, page 1-39	MEA (AIP), page 1-67	

Table 1-1   Alarm Index (continued)

FAILTOSW-PATH, page 1-40	MEA (EQPT), page 1-67	
FAILTOSWR, page 1-41	MEA (FAN), page 1-69	

1.2 Alarm Index by Alarm Type

The alarm index by alarm type gives the name and page number of every alarm in the chapter organized by alarm type.

Table 1-2   Alarm Index by Alarm Type

AIP::INVMACADDR, page 1-52
AIP::MEA (AIP), page 1-67
AIP::MFGMEM, page 1-70
BITS::AIS, page 1-9
BITS::LOF (BITS), page 1-53
BITS::LOS (BITS), page 1-60
BITS::SSM-FAIL, page 1-86
BPLANE::MFGMEM, page 1-70
DS1::AIS, page 1-9
DS1::LOF (DS1), page 1-53
DS1::LOS (DS-N), page 1-60
DS1::LPBKDS1FEAC, page 1-63
DS1::LPBKFACILITY (DS-N or EC1-12), page 1-63
DS1::LPBKTERMINAL (G1000-4), page 1-66
DS1::RCVR-MISS, page 1-76
DS1::TRMT, page 1-92
DS1::TRMT-MISS, page 1-93
DS3::AIS, page 1-9
DS3::DS3-MISM, page 1-33
DS3::FE-AIS, page 1-43
DS3::FE-DS1-MULTLOS, page 1-44
DS3::FE-DS1-SNGLLOS, page 1-44
DS3::FE-DS3-SA, page 1-45
DS3::FE-EQPT-NSA, page 1-45
DS3::FE-IDLE, page 1-46
DS3::FE-LOF, page 1-46
DS3::FE-LOS, page 1-47
DS3::LOF (DS3), page 1-54

Table 1-2   Alarm Index by Alarm Type

Table 1-2   Alarm Index by Alarm Type

EQPT::SWMTXMOD, page 1-87
EXT-SREF::SWTOPRI, page 1-88
EXT-SREF::SWTOSEC, page 1-88
EXT-SREF::SWTOTHIRD, page 1-89
EXT-SREF::SYNCPRI, page 1-89
EXT-SREF::SYNCSEC, page 1-89
EXT-SREF::SYNCTHIRD, page 1-90
FAN::EQPT-MISS, page 1-36
FAN::FAN, page 1-43
FAN::MEA (FAN), page 1-69
FAN::MFGMEM, page 1-70
G1000::CARLOSS (G1000-4), page 1-23
G1000::LPBKTERMINAL (G1000-4), page 1-66
G1000::RDI-P, page 1-77
G1000::TPTFAIL, page 1-91
NE::BLSROSYNC, page 1-19
NE::DATAFLT, page 1-33
NE::HITEMP, page 1-49
NE::PRC-DUPID, page 1-75
NE::RING-MISMATCH, page 1-78
NE::SYSBOOT, page 1-91
NE-SREF::FRNGSYNC, page 1-48
NE-SREF::FSTSYNC, page 1-48
NE-SREF::HLDOVERSYNC, page 1-49
NE-SREF::SWTOSEC, page 1-88
NE-SREF::SWTOTHIRD, page 1-89
NE-SREF::SYNCPRI, page 1-89
NE-SREF::SYNCSEC, page 1-89
NE-SREF::SYNCTHIRD, page 1-90
OCN::AIS-L, page 1-9
OCN::APSB, page 1-11
OCN::APSCDFLTK, page 1-11
OCN::APSC-IMP, page 1-13
OCN::APSCINCON, page 1-13
OCN::APSCM, page 1-14
OCN::APSCNMIS, page 1-14
OCN::APSMM, page 1-15

Table 1-2   Alarm Index by Alarm Type

OCN::AUTOLSROFF, page 1-16
OCN::EOC, page 1-33
OCN::E-W-MISMATCH, page 1-36
OCN::FEPRLF, page 1-47
OCN::FORCED-REQ, page 1-48
OCN::LOCKOUT-REQ, page 1-52
OCN::LOF (OC-N), page 1-55
OCN::LOS (OC-N), page 1-62
OCN::LPBKFACILITY (OC-N), page 1-64
OCN::LPBKTERMINAL (OC-N), page 1-66
OCN::SD-L, page 1-79
OCN::SF-L, page 1-81
OCN::SQUELCH, page 1-85
OCN::SSM-FAIL, page 1-86
OCN::STU, page 1-86
STSMON::AIS-P, page 1-10
STSMON::CONCAT, page 1-25
STSMON::AUTOSW-AIS, page 1-17
STSMON::AUTOSW-LOP (STSMON), page 1-17
STSMON::AUTOSW-PDI, page 1-18
STSMON::AUTOSW-SDBER, page 1-18
STSMON::AUTOSW-SFBER, page 1-18
STSMON::AUTOSW-UNEQ (STSMON), page 1-18
STSMON::FAILTOSW, page 1-39
STSMON::FORCED-REQ, page 1-48
STSMON::LOCKOUT-REQ, page 1-52
STSMON::LOP-P, page 1-58
STSMON::MAN-REQ, page 1-67
STSMON::PDI-P, page 1-72
STSMON::PLM-P, page 1-74
STSMON::RFI-P, page 1-77
STSMON::TIM-P, page 1-91
STSMON::UNEQ-P, page 1-93
STSTRM::LOP-P, page 1-58
STSTRM::PLM-P, page 1-74
STSTRM::SD-P, page 1-80
STSTRM::SF-P, page 1-82

Table 1-2   Alarm Index by Alarm Type

STSTRM::TIM-P, page 1-91
STSTRM::UNEQ-P, page 1-93
VT-MON::AIS-V, page 1-10
VT-MON::AUTOSW-AIS, page 1-17
VT-MON::AUTOSW-LOP (STSMON), page 1-17
VT-MON::AUTOSW-PDI, page 1-18
VT-MON::AUTOSW-SDBER, page 1-18
VT-MON::AUTOSW-SFBER, page 1-18
VT-MON::AUTOSW-UNEQ (STSMON), page 1-18
VT-MON::FORCED-REQ, page 1-48
VT-MON::LOCKOUT-REQ, page 1-52
VT-MON::LOP-V, page 1-59
VT-MON::UNEQ-V, page 1-94
VT-TERM::AIS-V, page 1-10
VT-TERM::LOP-V, page 1-59
VT-TERM::PLM-V, page 1-75
VT-TERM::RFI-V, page 1-78
VT-TERM::SD-P, page 1-80
VT-TERM::SF-P, page 1-82
VT-TERM::UNEQ-V, page 1-94

1.2.1 Alarm Type/Object Definition

Table 1-3   Alarm Type/Object Definition

AIP	Auxiliary interface protection module
BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)
BPLANE	The backplane
DS1	A DS1 line on a DS1 or DS3XM card
DS3	A DS3 line on a DS3 or DS3XM card
E1000F	An Ethernet line on an E1000 card
E100T	An Ethernet line on an E100 card
EC1-12	An EC1 line on an EC1 card
ENVALRM	An environmental alarm port on an AIC card
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, STS and VT
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2)
FAN	Fan-tray assembly

Table 1-3   Alarm Type/Object Definition

G1000	An Ethernet line on a G1000
NE	The entire network element (SYSTEM)
NE-SREF	Represents the timing status of the NE
OCN	An OCN line on an OCN card
RING	BLSR ring number (STSRNG)
STSMON	STS alarm detection at the monitor point (upstream of cross-connect)
STSTRM	STS alarm detection at termination (downstream of cross-connect)
VT-MON	VT1 alarm detection at the monitor point (upstream of cross-connect)
VT-TERM	VT1 alarm detection at termination (downstream of cross-connect)

1.3 Trouble Notifications

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 reports both alarmed trouble notifications, under the Alarms tab, and non-alarmed (NA) trouble notifications, under the Conditions tab in CTC. Alarms signify a problem that the user needs to fix, such as a loss of signal (LOS). Conditions notify the user of an event which does not require action, such as a switch to a secondary timing reference (SWTOSEC) or a user-initiated manual reset (MANRESET).

Telcordia further divides alarms into Service-Affecting (SA) and Non-Service-Affecting (NSA) status. An SA failure affects a provided service or the network's ability to provide service. For example, a missing transmitter (TRMT-MISS) alarm is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a port on an active DS1-14 card is removed. This affects a provided service, because traffic switches to the protect card. The high temperature (HITEMP) alarm, which means the ONS 15454 is hotter than 122 degrees Fahrenheit (50 degrees Celsius), is also an SA failure. Although for example a particular DS1-14 port may not be affected, a high temperature affects the network's ability to provide service.

1.3.1 Conditions

When an SA failure is detected, the ONS 15454 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 show up on the Conditions screen of the ONS 15454. However, unlike most conditions which are non-alarmed, Telcordia classifies these conditions as not reported (NR).

Both CTC and TL1 report NRs and NAs as conditions when conditions are retrieved. NAs are also reported as autonomous events under TL1 and under the History tab of the CTC. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 TL1 Command Guide*.

1.3.2 Severities

The ONS 15454 uses Tecordia-standard 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. For example, with a DS1-14 LOS, a Major alarm, 24 DS-0 circuits lose protection. But with a OC-192 LOS, a Critical alarm, over a hundred thousand DS-0 circuits lose protection.

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

Telcordia standard severities are the default settings for the ONS 15454. A user may customize ONS 15454 alarm severities with the alarm profiles feature. For a description of alarm profiles, refer to the *Cisco ONS 15454 Installation and Operations Guide*.

This chapter lists the default alarm severity for the active reporting card, if applicable. The default severity for alarms reported by standby cards is always Minor, Non-Service-Affecting.

1.4 Alarm Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description and troubleshooting procedure accompany each alarm and condition.

1.4.1 AIS

- Not Reported (NR)

The ONS 15454 detects an alarm indication signal (AIS) in the SONET overhead. This alarm 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 OC-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 may 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   Clear the upstream alarms.

1.4.2 AIS-L

- Not Reported (NR)

The ONS 15454 detects an alarm indication signal (AIS) in the SONET overhead. This alarm 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 OC-N port in-service. The upstream node often reports an LOS or has an out-of-service port. The AIS-L clears when you clear the primary alarm on the upstream node. However, the primary alarm node may not report any alarms that indicate it is at fault.

An AIS-L occurs at the line layer. The line layer refers to the segment between two SONET devices in the circuit and is also known as a maintenance span. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization.

Procedure: Clear the AIS-L Condition

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

Step 2   Clear the upstream alarms.

1.4.3 AIS-P

- Not Reported (NR) (Condition)

The ONS 15454 detects an alarm indication signal (AIS) in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. The AIS is caused by an incomplete circuit path, for example, when the port on the reporting node is in-service, but a node upstream on the circuit does not have its port in-service. The upstream node often reports a LOS or has an OC-N port out of service. The AIS-P clears when the primary alarm on the upstream node is cleared. However, the node with the primary alarm may not report any alarms to indicate it is at fault.

AIS-P occurs in each node on the incoming OC-N path. The path layer is the segment between the originating equipment and the terminating equipment. This path segment encompasses several consecutive line segments or segments between two SONET devices. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15454, often perform the origination and termination tasks of the SONET payload.

Procedure: Clear the AIS-P Condition

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

Step 2   Clear the upstream alarms.

1.4.4 AIS-V

- Not Reported (NR)

The ONS 15454 detects an alarm indication signal (AIS) in the SONET overhead. This alarm 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 OC-N port in-service. The upstream node often reports a LOS or has an out-of-service port. The AIS-V clears when the primary alarm is cleared. The node with the out-of-service port may not report any alarms to indicate it is at fault.

An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. The VT, or electrical layer, is created when the SONET signal is broken down into an electrical signal, for example when an optical signal comes into an ONS 15454 OC-N card. If this optical signal is demultiplexed by the ONS 15454, and one of the channels separated from the optical signal is then cross-connected into the DS1-14 ports in the same node, that ONS 15454 reports an AIS-V alarm.

An AIS-V error message on the electrical card is accompanied by an AIS-P error message on the cross-connected OC-N card.

Note   See the "AIS-V on DS3XM-6 Unused VT Circuits" section on page 2-33 for AIS-Vs that occur on DS3XM-6 unused VT circuits.

Procedure: Clear the AIS-V Condition

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

Step 2   Correct the upstream alarms.

1.4.5 APSB

- Minor, Non-service affecting

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 SONET nodes send invalid APS codes if configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15454. These invalid codes will raise an APSB on an ONS node.

Procedure: Clear the APSB Alarm

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

Step 2   If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment may not interoperate effectively with the ONS 15454. For ONS 15454 protection switching to operate properly, the upstream equipment may need to be replaced.

1.4.6 APSCDFLTK

- Minor, Non-service affecting

The Default K Byte Received alarm occurs when a BLSR is not properly configured, for example, when a four-node BLSR has one node configured as UPSR. A node in a UPSR or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

The alarm can also be caused when a new node is added but a new ring map has not been accepted. Troubleshooting for APSCDFLTK is often similar to troubleshooting for BLSROSYNC.

Procedure: Clear the APSCDFLTK Alarm

Step 1   Prior to accepting a new mapping table, verify that each node has a unique node ID number.

   a.   Log into a node on the ring.

   b.   Click the **Provisioning > Ring** tabs.

   c.   Record the node ID number.

   d.   Repeat steps a – c for all nodes in the ring.

   e.   If two nodes have the same node ID number, change one node's ID number so that each node has a unique node ID.

   f.   Click **Apply**.

Step 2   Verify correct configuration of east port and west port optical fibers (see the "E-W-MISMATCH" section on page 1-36).

Step 3   If it is a four fiber BLSR 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 there is a working fiber incorrectly attached to a protection fiber.

Step 4   Click **Yes** to accept the Ring Map.

Step 5   If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.

   a.   At the node (default) view, click the **Provisioning > Ring** tabs.

   b.   Highlight a BLSR ring.

   c.   Click **Ring Map**.

   d.   Verify that each node that is part of the ring appears on the Ring Map with a Node ID and IP Address.

   e.   Click **Close**.

Step 6   If nodes are not visible, ensure that SDCC terminations exist on each node.

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

   b.   Click **Create**.

   c.   Click the OC-N card that links to the adjacent node.

   d.   Click **OK**.

Step 7   If the alarm still does not clear, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.7 APSC-IMP

- Minor, Non-service affecting

An Improper SONET Automatic Protect Switch code alarm indicates invalid K bytes. This alarm occurs on OC-N cards in a BLSR 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. APSCIMP 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the APSC-IMP Alarm

Step 1   To determine the validity of the K byte signal, examine the received signal. Use an optical test set capable of viewing SONET overhead.

Step 2   If the K byte is invalid, the problem lies in upstream equipment and not in the reporting ONS 15454. Troubleshoot the appropriate upstream equipment.

Step 3   If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs:

   a.   Using CTC, log into a node on the ring.

   b.   Click the **Provisioning > Ring** tabs.

   c.   Record the ring ID number.

   d.   Repeat steps a – c for all nodes in the ring.

Step 4   If a node has a ring ID number that does not match the other nodes, change the ring ID number of that node to match the other nodes in the ring.

Step 5   Click **Apply**.

1.4.8 APSCINCON

- Minor, Service affecting

An inconsistent automatic protection switching (APS) alarm is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454, to switch the SONET signal from a working to a protect path. 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

Step 1   Look for other alarms, especially LOS, loss of frame (LOF) or AIS. Clearing these alarms clears the APSCINCON alarm.

Step 2   If an APSINCON alarm occurs with no other alarms, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.9 APSCM

- Major, Service affecting

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

⚠
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.**

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

Procedure: Clear the APSCM Alarm

Step 1   Verify that the working-card channel fibers connect directly to the adjoining node's working-card channel fibers.

Step 2   Verify that the protection-card channel fibers connect directly to the adjoining node's protection-card channel fibers.

1.4.10 APSCNMIS

- Major, Service affecting

The APS 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 may occur and clear when a BLSR is being provisioned. If so the user can disregard the temporary occurrence. If an APSCNMIS raises and stays, the alarm clears when the receiving node receives or matches the expected K-byte. If the APSCNMIS is raised and stays, the alarm clears when a K byte with valid source node ID in K2 is received.

Procedure: Clear the APSCNMIS Alarm

Step 1   Verify that each node has a unique node ID number.

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

    b. Click the BLSR row to highlight.

    c. Click **Ring Map**.

    d. If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.

    e. Click **Close** on the Ring Map dialog box.

Step 2   If two nodes have the same node ID number, change one node's ID number so that each node has a unique node ID:

    a. Display the network view.

    b. Log into one of the nodes that uses the repeated node ID recorded in Step 1.

> ✎
>
> **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 > Ring** tabs. This screen displays the node ID of the node you are logged into.

    c. Click the Node ID table cell to reveal a pull-down menu.

    d. Select a unique node ID from the pull-down menu and click **Apply**.

> ✎
>
> **Note**   Locking out and clearing the lockout on a span causes the ONS 15454 to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

Step 3   If the alarm does not clear, lockout a span on the ring and then clear the lockout:

    a. Click the **Ring > Maintenance** tabs.

    b. Click the table cell under the West Switch heading to reveal the pull-down menu.

    c. Select **LOCKOUT SPAN** and click **Apply**.

    d. Click **OK** on the BLSR Operations dialog box.

    e. Click the same table cell under the West Switch heading to reveal the pull-down menu.

    f. Select **CLEAR** and click **Apply**.

    g. Click **OK** on the BLSR Operations dialog box.

1.4.11 APSMM

- Minor, Non-service affecting

An APS Mode Mismatch failure occurs when there is a mismatch of the protection switching schemes at the two ends of the span. If one node is provisioned for bidirectional switching, the node at the other end of the span must also be provisioned for bidirectional switching. If one end is provisioned for bidirectional and the other is provisioned for unidirectional, an APSMM alarm occurs in the ONS node that is provisioned for bidirectional. This alarm occurs in a 1+1 configuration.

Procedure: Clear the APSMM Alarm

Step 1 For the reporting ONS 15454, display the CTC node view and click the **Provisioning > Protection** tabs.

Step 2 Choose the 1+1 protection group configured for the OC-N cards.

This is the protection group optically connected (with DCC connectivity) to the far end.

Step 3 Record whether the bidirectional switching box is checked.

Step 4 Log into the far end node and verify that the OC-N 1+1 protection group is provisioned.

This is the protection group optically connected (with DCC connectivity) to the near end.

Step 5 Verify that the bidirectional switching box matches the checked or unchecked condition of the box recorded in Step 3. If not, change it to match.

Step 6 Click **Apply**.

1.4.12 AUTOLSROFF

- Critical, Service affecting

⚠ **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.**

The auto laser off alarm raises when the OC-192 card temperature exceeds 90 degrees Centigrade. The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.

Procedure: Clear the AUTOLSROFF Alarm

Step 1 Read the temperature displayed on the ONS 15454 LCD front panel.

Step 2 If the temperature of the ONS 15454 exceeds 90 degrees Centigrade, complete the "Clear the HITEMP Alarm" procedure on page 1-49.

Step 3 If the temperature of the ONS 15454 is below 90 degrees Centigrade, replace the OC-192 card.

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

Step 4   Call the Technical Assistance Center (TAC) at 1-800-553-2447 to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

1.4.13 AUTORESET

- Minor, Non-service affecting

The AUTORESET alarm occurs when a card performs a warm reboot automatically. This happens 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the AUTORESET Alarm

Step 1   Check for additional alarms that may 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.

✎

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

1.4.14 AUTOSW-AIS

- Not Reported (Condition)

AUTOSW-AIS indicates that automatic UPSR protection switching took place because of an AIS alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "AIS" section on page 1-9.

1.4.15 AUTOSW-LOP (STSMON)

- Not Alarmed (Condition)

AUTOSW-LOP indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "LOP-P" section on page 1-58.

1.4.16 AUTOSW-LOP (VT-MON)

- Minor, Service affecting

AUTOSW-LOP indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "LOP-P" section on page 1-58.

1.4.17 AUTOSW-PDI

- Not Alarmed (Condition)

AUTOSW-PDI indicates that automatic UPSR protection switching took place because of a PDI alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "PDI-P" section on page 1-72.

1.4.18 AUTOSW-SDBER

- Not Alarmed (NA) (Condition)

AUTOSW-SDBER indicates that automatic UPSR protection switching took place because of an SD alarm. The UPSR is configured for revertive switching and has switched back to the working path.

1.4.19 AUTOSW-SFBER

- Not Alarmed (NA) (Condition)

AUTOSW-SFBER indicates that automatic UPSR protection switching took place because of a SF alarm. The UPSR is configured for revertive switching and will switch back to the working path. Troubleshoot with the "SF-L" section on page 1-81.

1.4.20 AUTOSW-UNEQ (STSMON)

- Not Alarmed (Condition)

AUTOSW-UNEQ indicates that automatic UPSR protection switching took place because of an UNEQ alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "UNEQ-P" section on page 1-93.

1.4.21 AUTOSW-UNEQ (VT-MON)

- Minor, Service affecting

AUTOSW-UNEQ indicates that automatic UPSR protection switching took place because of an UNEQ alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the "UNEQ-P" section on page 1-93.

1.4.22 BKUPMEMP

- Critical, Non-service affecting

The BKUPMEMP alarm refers to a problem with the TCC+ card's flash memory. The alarm occurs when the TCC+ 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+.

The BKUPMEMP alarm will also raise the EQPT alarm. In this instance, use the following procedure will clear the BKUPMEMP and the EQPT alarm.

Procedure: Clear the BKUPMEMP Alarm

Step 1   Verify that both TCC+ cards are powered and enabled by confirming lighted ACT/STBY LEDs on the TCC+ cards.

Step 2   Reset the active TCC+ card to make the standby TCC+ card active:

   a. In CTC, display the node view.

   b. Position the cursor over the active TCC+ card slot.

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

Step 3   If the alarm clears, reseat the old TCC+ and allow it to boot up completely.

Step 4   Do a second reset, this time on the newly-active TCC+ card to make the recently-reseated standby TCC+ card active.

   a. In CTC, display the node view.

   b. Position the cursor over the active TCC+ card slot.

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

Step 5   If the alarm reappears after you perform the switch, replace the TCC+ card.

   a. Open the card ejectors.

   b. Slide the card out of the slot.

   c. Open the ejectors on the replacement card.

   d. Slide the replacement card into the slot along the guide rails.

   e. Close the ejectors.

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

1.4.23 BLSROSYNC

   • Major, Service affecting

The BLSR Out Of Sync alarm occurs when the mapping table needs updating. To clear the alarm, a new ring map must be created and accepted. Before you create a new ring map, complete Steps 1 – 4.

Cisco ONS 15454 Troubleshooting and Maintenance Guide, R3.2

Procedure: Clear the BLSROSYNC Alarm

Step 1   Prior to accepting a new mapping table, verify that each node has a unique node ID number:

   a.   Log into a node on the ring.

   b.   Click the **Provisioning > Ring** tabs.

   c.   Record the Node ID number.

   d.   Repeat steps a – c for all nodes in the ring.

   e.   If two nodes have the same node ID number, change one node ID number, so the node ID number is unique within that ring.

   f.   Click **Apply**.

Step 2   Verify that each node has a ring ID that matches the other node ring IDs:

   a.   Log into the next node on the ring.

   b.   Click the **Provisioning > Ring** tabs.

   c.   Record the Ring ID number.

   d.   Repeat steps a – b for all nodes in the ring.

   e.   If a node has a ring ID number that does not match the other nodes, change the ring ID to match all the other nodes in the ring.

   f.   Click **Apply**.

Step 3   Verify correct configuration of the east port and west port optical fibers (see the "E-W-MISMATCH" section on page 1-36.)

Step 4   If it is a four-fiber BLSR system, amke sure that each protect fiber connects to another protect fiber, and each working fiber connects to another working fiber. The software does not report any alarm, if there is a working fiber misconnected to a protect fiber.

Step 5   If the east-to-west configuration changes, click **Apply**.

   The BLSR Ring Map Change screen appears.

Step 6   Click **Yes** to accept the Ring Map.

Step 7   If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.

Step 8   If nodes are not visible, ensure that SDCC terminations exist on each node.

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

   b.   Click **Create**.

   c.   Click the OC-N card that links to the adjacent node.

   d.   Click **OK**.

Step 9   If alarms are raised when the DCCs are turned on, follow the troubleshooting procedure in the "EOC" section on page 1-33.

Step 10   If the alarm still does not clear, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.24 CARLOSS (E-Series)

- Major, Service affecting

A carrier loss on the LAN is the data equivalent of a SONET 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 cable, an OC-N fiber connected to the Ethernet GBIC 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's 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 the G1000-4 card, as this card does not use STP and is unaffected by STP reestablishment.

⚠

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

Procedure: Clear the CARLOSS Alarm

Step 1   Verify that the Ethernet cable is properly connected and attached to the correct port.

Step 2   Verify that the Ethernet cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3   Check that the transmitting device is operational. If not, troubleshoot the device.

Step 4   Using a test set, determine that a valid signal is coming into the Ethernet port.

Step 5   If a valid Ethernet signal is not present and the transmitting device is operational, replace the Ethernet cable connecting the transmitting device to the Ethernet port.

Step 6   If a valid Ethernet signal is present, physically reseat the Ethernet card.

Step 7   If the alarm does not clear, replace the Ethernet card.

    a.   Open the card ejectors.

    b.   Slide the card out of the slot.

    c.   Open the ejectors on the replacement card.

    d.   Slide the replacement card into the slot along the guide rails.

    e.   Close the ejectors.

    ✎

    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, 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 may 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 15454s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

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

b.   Right-click or left-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 and card that host the Ethernet circuit at the other end of the Ethernet manual cross connect.

e.   Log into the ONS 15454 at the other end of the Ethernet manual cross connect.

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

g.   Click the **Circuits** tab.

h.   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 OC-N card on the same node.

i.   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.

j.   If one of the circuit sizes is incorrect, navigate to the incorrectly configured circuit.

k.   Click the incorrectly configured circuit to highlight it and click **Delete**.

l.   Click **Yes** at the Delete Circuit dialog box, and **OK** at the Confirmation dialog box.

m.   Reconfigure the circuit with the correct circuit size. Refer to the Cisco Installation and Operations Guide for procedures to provision Ethernet manual cross connects.

1.4.25 CARLOSS (EQPT)

- Minor, Non-service affecting

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

Procedure: Clear the CARLOSS Alarm

Step 1   Verify connectivity by pinging the ONS 15454 that is reporting the alarm:

a.   If you are using a Microsoft Windows operating system, from the Start Menu choose **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, 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 the 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.

1.4.26 CARLOSS (G1000-4)

- Major, Service affecting

A carrier loss on the LAN is the data equivalent of a SONET LOS alarm. The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-4 stems from two general areas:

a) The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. A common cause is an Ethernet cable not connected properly to the reporting Ethernet port, an OC-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.

b) There is a problem in the end-to-end path (including possibly the remote end G1000-4 card), which 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 will normally be accompanied by another alarm or condition on the end-to-end path, such as a TPTFAIL or an OC-N alarm or condition.

Refer to the Ethernet Operations Chapter of the Installation and Operations Guide for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TPTFAIL" section on page 1-91 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CARLOSS Alarm

Step 1   Verify that the Ethernet cable is properly connected and attached to the correct port.

Step 2   Verify that the Ethernet cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3   Check that the transmitting attached Ethernet device is operational. If not, troubleshoot the device.

Step 4   Using an Ethernet test set, determine that a valid signal is coming into the Ethernet port.

Step 5   If a valid Ethernet signal is not present and the transmitting device is operational, replace the Ethernet cable connecting the transmitting device to the Ethernet port.

Step 6   If link auto negotiation is set to enabled on the G1000-4 port, but the auto negotiation process fails then the G1000-4 will turn off its transmitter laser and report a CARLOSS alarm. If link auto negotiation has been enabled on the port, check for conditions which could cause auto negotiation to fail:

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

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

Step 7   If all above attempts fail, disable and re-enable the Ethernet port to attempt to remove the CARLOSS condition (this will restart the auto negotiation process).

Step 8   If the TPTFAIL alarm is also reported, see "TPTFAIL" section on page 1-91. If the TPTFAIL alarm is not reported, continue to the next step.

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

Step 9   Check to see if terminal loopback has been provisioned on this port.

On the G1000-4 card, provisioning a terminal loopback causes the transmit laser to turnoff. 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. Shutting of the transmit laser could cause the CARLOSS alarm detected by the G1000-4 port in loopback.

a.   Click the **Conditions** tab click **Retrieve Conditions**.

b.   If LPBKTERMINAL appears in the condition field of the Conditions pane, a terminal loopback has been set on this port.

Click **Maintenance > Loopback**.

Under the Loopback Type column, select NONE for the port row reporting the alarm.

Click **Apply**.

c.   If LPBKTERMINAL does not appear in the condition field of the Conditions pane, continue to Step 4.

Step 10   If a CARLOSS alarm repeatedly appears and clears, 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 may 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 15454s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

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

b.   Right-click or left-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 and card that host the Ethernet circuit at the other end of the Ethernet manual cross connect.

    e. Log into the ONS 15454 at the other end of the Ethernet manual cross connect.

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

    g. Click the **Circuits** tab.

    h. 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 OC-N card on the same node.

    i. 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.

    j. If one of the circuit sizes is incorrect, navigate to the incorrectly configured circuit.

    k. Click the incorrectly configured circuit to highlight it and click **Delete**.

    l. Click **Yes** at the Delete Circuit dialog box, and **OK** at the Confirmation dialog box.

    m. Reconfigure the circuit with the correct circuit size. Refer to the Cisco Installation and Operations Guide for procedures to provision Ethernet manual cross connects.

Step 11   If a valid Ethernet signal is present, physically reseat the Ethernet card.

Step 12   If the alarm does not clear, replace the Ethernet card.

    a. Open the card ejectors.

    b. Slide the card out of the slot.

    c. Open the ejectors on the replacement card.

    d. Slide the replacement card into the slot along the guide rails.

    e. Close the ejectors.

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

1.4.27 CONCAT

- Critical, Service affecting

The STS Concatenation error alarm occurs when the transmitted STSc circuit is smaller than the provisioned STSc, which causes a mismatch of the circuit type on the concatenation facility. For example, an STS3c or STS1 is sent across a circuit provisioned for STS12c.

Either an incorrect circuit size was provisioned on the reporting node, or the circuit source is delivering the wrong circuit size. If a recently-configured circuit reports this alarm, it is more likely that the provisioned circuit size is incorrect. If a previously configured circuit has been operating correctly for a period and then reports the alarm, it is more likely that a problem occurred with the circuit source.

Procedure: Clear the CONCAT Alarm

Step 1   Check that the provisioned circuit size is correct:

   a.   Click the **Circuits** tab.

   b.   Find the appropriate row using the Circuit Name and record the size listed in the size column.

   c.   Determine whether the size listed matches the original network design plan.

Step 2   If the circuit size listed does not match the original network design plan, delete the circuit:

   a.   Click the circuit row to highlight it and click **Delete**.

   b.   Click **Yes** at the Delete Circuits dialog box.

   c.   Recreate the circuit with the correct circuit size.

Step 3   Check that the size of the circuit source matches the correct circuit size:

   a.   Measuring the source signal with a test set to determine if the circuit size matches the provisioned circuit.

   b.   If the source circuit signal is a test set, check that the test set settings match the intended circuit size.

1.4.28 CONTBUS-A

   • Major, Non-service affecting

The communication failure TCC A to shelf slot alarm means the TCC+ card in Slot 7 has lost communication with a line card. Cards require frequent communication with the TCC+ card because the TCC+ performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET Data Communications Channel (SDCC) termination, system fault detection, and other operations for the ONS 15454. The TCC+ card also ensures that the system maintains Telcordia timing requirements.

The CONTBUS-A alarm can appear briefly when the ONS 15454 switches to the standby TCC+ card. In this instance, the alarm clears after the cards establish communication with the new primary TCC+ card. In cases where the alarm persists, the problem lies in the physical path of communication from the TCC+ to the reporting card. The physical path of communication includes the TCC+ card, the card in Slot *X* and the backplane.

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

Procedure: Clear the CONTBUS-A Alarm

Step 1   Ensure the reporting card is physically present. Record the card type.

Step 2   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 1-67.

Step 3   If only one card slot reporting the alarm, perform a software reset of the traffic card:

    a.   Display the CTC node view.

    b.   Position the cursor over the slot reporting the alarm.

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

Step 4   If the software reset does not clear the alarm, physically reseat the reporting card.

Step 5   If all traffic cards report this alarm, perform a software reset of the active TCC+ card.

    a.   Display the node view.

    b.   Position the cursor over the active TCC+ card slot.

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

Step 6   If the software reset does not clear the alarm, physically reseat the TCC+ card.

Step 7   If the alarm still does not clear, replace the TCC+ card.

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

1.4.29 CONTBUS-A-18

- Major, Non-service affecting

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

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

Procedure: Clear the CONTBUS-A-18 Alarm

Step 1   Position the cursor over the TCC+ card in Slot 7.

Step 2   Right-click the mouse to reveal a menu.

Step 3   To clear the alarm, choose **RESET CARD** to make the standby TCC+ in Slot 11 the active TCC+ and clear the alarm.

Step 4   Wait approximately 2 minutes for the TCC+ in Slot 7 to reset as the standby TCC+. Verify that the Standby LED is lit before proceeding to the next step.

Step 5   Position the cursor over the TCC+ card in Slot 11.

Step 6   Right-click the mouse to reveal a menu.

Step 7   Choose **RESET CARD** to make the standby TCC+ in Slot 7 the active TCC+.

Step 8   If the alarm reappears when the TCC+ in Slot 7 reboots as the active TCC+, the TCC+ card in Slot 7 is defective and must be replaced.

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

1.4.30 CONTBUS-B

- Major, Non-service affecting

The communication failure TCC A to shelf slot alarm means the TCC+ card in Slot 11 lost communication with a line card. Cards require frequent communication with the TCC+ card, because the TCC+ card performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET DCC termination, and system fault detection among other operations for the ONS 15454. The TCC+ card also ensures that the system maintains Telcordia timing requirements.

This alarm may appear briefly when the ONS 15454 switches over to the protect TCC+ card. In this instance, the alarm clears after the other cards establish communication with the new primary TCC+ card. In cases where the alarm persists, the problem lies in the physical path of communication from the TCC+ card to the reporting card. The physical path of communication includes the TCC+ card, the card in Slot *X,* and the backplane.

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

Procedure: Clear the CONTBUS-B

Step 1   Ensure the reporting card is physically present and that it matches the type of card identified in that slot on CTC.

Step 2   If this slot is the only one reporting the alarm, perform a software reset of the traffic card:

   a. Display the CTC node view.

   b. Position the cursor over the slot reporting the alarm.

   c. Right-click the mouse and choose **RESET CARD** to do a software reset.

Step 3   If the software reset does not clear the alarm, physically reseat the reporting card.

Step 4   If all cards with the exception of the active TCC+ report this alarm, perform a software reset of the active TCC+:

   a. Display the CTC node view.

   b. Position the cursor over the active TCC+ card slot.

   c. Choose **RESET CARD**.

Step 5   If the software reset does not clear the card, physically reseat the TCC+ card to perform a card pull.

Step 6   If the alarm still does not clear, replace the TCC+ card.

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

1.4.31 CONTBUS-B-18

- Major, Non-service affecting

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

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

Procedure: Clear the CONTBUS-B-18 Alarm

Step 1   Position the cursor over the TCC+ card in Slot 11.

Step 2   Right-click and choose **RESET CARD** to make the TCC+ in Slot 11 the active TCC+ card.

Step 3   Wait approximately 2 minutes for the TCC+ in Slot 7 to reset as the standby TCC+ card. Verify that the Standby LED is lit before proceeding to the next step.

Step 4   Position the cursor over the TCC+ card in Slot 7.

Step 5   Right-click and choose **RESET CARD** again to make the TCC+ in Slot 11 the active TCC+ card.

Step 6   If the alarm reappears when the TCC+ in Slot 11 reboots as the active TCC+, the TCC+ card in Slot 11 is defective and must be replaced.

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

1.4.32 CTNEQPT-PBSTBY

- Critical, Service affecting

The interconnection equipment failure protect payload bus alarm indicates a failure of the main payload between the protect cross-connect (XC/XCVT/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, the TCC+ card or the backplane.

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

✎
Note   If CTNEQPT-PBSTBY is raised against all traffic cards on the shelf and SWMTXMOD, SD-L, AIS-L and RFI-L are also present, this could indicate a failed cross-connect card oscillator. Refer to the "Operation: Cross-Connect Card Oscillator Fails" section on page 2-31.

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

Procedure: Clear the CTNEQPT-PBSTBY Alarm

Step 1   Perform a software reset on the standby cross-connect (XC/XCVT/XC10G) card:

    a. Display the node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 2   If the alarm persists, physically reseat the standby cross-connect card.

Step 3   If the alarm persists and the reporting traffic card is the active card in the protection group, do a force switch to move traffic away from the card:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Click the Protect/Standby card of the selected groups.

    d. Click **Force** and **OK**.

Step 4   Perform a software reset on the reporting card:

    a. Display the CTC node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 5   If the alarm persists, physically reseat the reporting card.

Step 6   Clear the force switch:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Highlight either selected group.

    d. Click **Clear** and click **YES** at the confirmation dialog box.

Step 7   If the reporting traffic card is protect, perform a software reset on the reporting card:

    a. Display the CTC node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 8   If the alarm persists, physically reseat the reporting card.

Step 9   If the alarm persists, replace the standby cross-connect card.

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

Step 10   If the alarm persists, replace the reporting traffic card.

1.4.33 CTNEQPT-PBACT

- Critical, Service affecting

The interconnection equipment failure protect payload bus alarm indicates a failure in the main payload bus between the active cross-connect (XC/XCVT/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+ card, as shown in Step 1, and physically reseat this TCC+ card. If this fails to clear the alarm, replace the TCC+ card. Do not physically reseat an active TCC+ card; this disrupts traffic.

> **Note**   If CTNEQPT-PBACT is raised against all traffic cards on the shelf and SWMTXMOD, SD-L, AIS-L and RFI-L are also present, this could indicate a failed cross-connect card oscillator. Refer to the "Operation: Cross-Connect Card Oscillator Fails" section on page 2-31

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

Procedure: Clear the CTNEQPT-PBACT Alarm

Step 1   Do a side switch from the active cross-connect (XC/XCVT/XC10G) card to the protect cross-connect card:

a. 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.

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

c. Click **Switch**.

    d. Click **Yes** on 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 2   Perform a software reset on the reporting card:

    a. From the node view, position the cursor over the slot reporting the alarm.

    b. Right-click to choose **RESET CARD**.

Step 3   If the alarm persists, perform a card pull on the standby cross-connect card.

Step 4   If the alarm persists and the reporting traffic card is the active card in the protection group, do a force switch to move traffic away from the card:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Click the Protect/Standby card of the selected groups.

    d. Click **Force** and **OK**.

Step 5   Perform a software reset on the reporting card:

    a. Display the CTC node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 6   If the alarm persists, physically reseat the reporting card.

Step 7   Clear the force switch:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Highlight either selected group.

Step 8   Click **Clear** and click **YES** at the confirmation dialog box.

Step 9   If the reporting traffic card is protect, perform a software reset on the reporting card:

    a. Display the CTC node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 10   If the alarm persists, physically reseat the reporting card.

Step 11   If the alarm persists, replace the cross-connect card. First, ensure the card has been side switched from active to standby (Step 1):

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

Step 12   If the alarm persists, replace the reporting traffic card.

1.4.34 DATAFLT

- Minor, Non-service affecting

The software fault data integrity fault alarm means the database exceeded the capacity of the flash memory on the TCC+.

⚠️

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

Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.35 DS3-MISM

- Not Alarmed (NA) (Condition)

The DS3 frame format mismatch indicates a frame format mismatch on the DS3-12E card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type is set to C-BIT for a DS3-12E card, and the incoming signal's frame format is detected as M23 or UNFRAMED, then the ONS 15454 reports a DS3-MISM alarm. The alarm is not raised when the line type is set to AUTO PROVISION or UNFRAMED.

The alarm or condition clears when the line type is set to AUTO PROVISION or UNFRAMED, the port state is set to OOS, or the correct frame format is set. Setting the line type to AUTO PROVIS ION causes the ONS 15454 to detect the received frame format and provision the port to use the matching frame format, either Unframed, M23 or C-bit.

Procedure: Clear the DS3-MISM

Step 1   Go to the CTC card-level view for the reporting DS3-12E.

Step 2   Click **Provisioning > Line** tabs.

Step 3   For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal.

Step 4   If the Line Type pull-down column does not to match the expected incoming signal, select the correct Line Type on the pull down menu.

Step 5   Click **Apply**.

Step 6   If the alarm does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use a test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal.

1.4.36 EOC

- Major, Non-service affecting

The termination failure SDCC alarm means the ONS 15454 has lost its data communications channel (DCC). The DCC is three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P.) The ONS 15454 uses the DCC on the SONET section layer (SDCC) to communicate network management information.

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.**

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

Procedure: Clear the EOC Alarm

Step 1   If an LOS alarm is also reported, first resolve the LOS alarm by following the troubleshooting procedure given for that alarm.

Step 2   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   Verify that both ends of the fiber span have in-service ports by checking that the ACT LED on each OC-N card is illuminated.

Step 4   Verify that the DCC is provisioned for the ports at both ends of the fiber span.

    a.   Under the node view, click the **Provisioning > SONET DCC** tabs.

    b.   If the slot and port are listed under **SDCC Terminations**, the DCC is provisioned.

    c.   If the slot and port are not listed under the SDCC Terminations, click **Create**.

    d.   Click the OC-N card that links to the adjacent node.

    e.   Click **OK**.

    f.   Repeat steps (a) – (e) at the adjacent nodes.

Step 5   Verify that the OC-N port is active and in-service:

    a.   Confirm that the OC-N card shows a green LED by viewing the 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 OC-N port is in In Service, double-click the card in the CTC to display the card-level view.

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

    d.   Verify that the Status column lists the port as In Service.

    e.   If the Status column lists the port as Out of Service, click the column and select **In Service**. Click **Apply**.

Step 6   With a test set, check for signal failures on fiber terminations.

Caution   Using a test set will disrupt service on the OC-N card. It may be necessary to manually switch traffic carrying circuits over to a protection path.

Step 7 Measure power levels to verify that the budget loss is within the parameters of the receiver. See the "Optical Card Transmit and Receive Levels" section on page 2-43.

Step 8 Ensure that fiber connectors are securely fastened and properly terminated.

Step 9 Reset the active TCC+ using the "Card Replacement" section on page 3-19.

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

Step 10 Replace the original active TCC+ with a new TCC+ card.

⚠

Caution Resetting the active TCC+ can result in loss of traffic.

Step 11 Delete and recreate the problematic SDCC termination:

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

   b. Highlight the problematic SDCC termination.

   c. Click **Delete**.

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

Step 12 Verify that both ends of the SDCC have been recreated at the optical ports.

Step 13 Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.37 EQPT

- Critical, Service affecting

An equipment failure (EQPT) alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BKUPMEMP alarm, follow the procedure "Clear the BKUPMEMP Alarm" section on page 1-19. This procedure will also clear the EQPT alarm.

⚠

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

Procedure: Clear the EQPT Alarm

Step 1 Perform a software reset on the reporting card.

   a. Display the CTC node view.

   b. Position the CTC cursor over the slot reporting the alarm.

   c. Right click **RESET CARD**.

Step 2 If the software reset fails to clear the alarm, physically reseat the card.

Step 3 If the physical reseat of the card fails to clear the alarm, replace the card.

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

1.4.38 EQPT-MISS

- Critical, Service affecting

The rplaceable equipment unit is missing alarm is reported against the fan tray assembly unit. It indicates the 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. Plug the wristband cable into the ESD jack located on the lower-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, use the retractable handles embedded in the front of the fan tray to pull the fan tray assembly forward several inches and the push the fan tray assembly firmly back into the ONS 15454 shelf assembly and close the retractable handles.

Step 3   If no fan try assembly is present, obtain a fan tray assembly and refer to the fan tray assembly installation information in the Cisco ONS 15454 Installation and Operations Guide.

1.4.39 E-W-MISMATCH

- Major, Service affecting

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 hook up the fibers correctly, or the ring provisioning plan was flawed. You can physically reconnect the 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. The CTC method will clear the alarm, but may change the traditional east-west node connection pattern of the ring.

> ✎
> **Note**   The E-W-MISMATCH alarm also appears during the initial set up of a ring with its East-West 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 labelled as the west slot and the higher numbered slot is labelled 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 screen's network map.

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

Step 4   Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 - Node2/Slot6/Port1 (2F BLSR OC48, Ring ID=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as `Slot 12/Port 1`. Label the Node 2 end of that same span *Slot 6/ Port 1*.

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

Step 6   Label the highest slot at each node *east* and the lowest 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-east or west-to-west connection, physically switch the fiber 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 above 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.

Procedure: Clear the E-W-MISMATCH Alarm with the 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 > Ring** tabs.

Step 3   From the row of information for the fiber span, write down the Node ID, Ring ID, and the Slot and Port in the east line list and west line list.

Step 4   Click the row from Step 3 to select it and click **Delete**.

Step 5   Click **Create**.

Step 6   Fill in the Ring ID and Node ID from the information collected in Step 3.

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   Click **Yes** at the Ring Map Change dialog box.

Step 11   Click **Accept** at the new Ring Map.

1.4.40 EXCCOL

- Minor, Non-service affecting

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

Procedure: Clear the EXCCOL Alarm

Troubleshoot the network management LAN connected to the TCC+ card for excess collisions. You may 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+ card has a flow rate set to 10 Mb, half-duplex.

Step 2 Troubleshoot the network device connected to the TCC+ card and the network management LAN.

1.4.41 EXERCISE-RING-FAIL

- Not Alarmed (NA) (Condition)

The Exercise-Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The EXERCISE-RING-FAIL condition is raised if the command was issued and accepted but the exercise did not take place.

Note If the exercise command gets rejected due to the existence of a higher priority condition in the ring, EXERCISE-RING-FAIL will not be reported.

Procedure: Clear the EXERCISE-RING-FAIL Condition

Step 1 Check for any LOS, LOF or BLSR service affecting alarms.

Step 2 Lookup and troubleshoot any of these alarms, then reissue the Exercise-Ring command.

1.4.42 EXERCISE-SPAN-FAIL

- Not Alarmed (NA) (Condition)

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISE-SPAN-FAILED alarm is raised if the command was issued and accepted but the exercise did not take place.

> **Note**   If the exercise command gets rejected due to the existence of a higher priority condition in the span, EXERCISE-SPAN-FAIL will not be reported.

Procedure: Clear the EXERCISE-SPAN-FAIL Condition

Step 1   Check for any LOS, LOF or BLSR service affecting alarms.

Step 2   Lookup and troubleshoot any of these alarms, then reissue the Exercise Span command.

1.4.43 EXT

- Minor, Service affecting

An external facility alarm is detected external to the node because an environmental alarm is present, for example, a door is open or flooding has occurred.

Procedure: Clear the EXT Alarm

Step 1   Open the AIC card maintenance screen to gather further information about this alarm.

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

1.4.44 FAILTOSW

- Not Alarmed (NA) (Condition)

The FAILTOSW alarm is raised when a working DS-N card cannot switch to the protect card in a 1:N protection group, because another working DS-N card, with a higher-priority alarm, is switched over and monopolizing the lone protect card.

Procedure: Clear the FAILTOSW Alarm

Step 1   Lookup and troubleshoot the higher-priority alarm. Clearing this alarm will free up the 1:N card and clear the FAILTOSW.

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

Step 2   Replace the working DS-N card that is reporting the higher-priority alarm. This card is the working DS-N card using the DS:N card protection and not reporting FAILTOSW.

Replacing the working DS-N card reporting the higher-priority alarm, will allow 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.

1.4.45 FAILTOSW-PATH

- Not Alarmed (NA) (Condition)

The fail to switch path means the working path did not switch to the protection path on a UPSR. Common causes of this alarm include a missing or defective protection card or a lockout set on one of the UPSR nodes.

⚠

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

Procedure: Clear the FAILTOSW-PATH on a UPSR Configuration

Step 1   Ensure that a lockout is not set on the UPSR:

   a.   Display the CTC network view.

   b.   Right-click the span (the line between the nodes).

   c.   Click **Circuits**.

   d.   Under Switch State, confirm that Clear appears.

   e.   If Clear does appear, perform Steps a – d at the next span.

   f.   If Clear still does not appear, click the **Switch all UPSR- circuits away** menu.

   g.   Choose **Clear** and click **Apply**.

   h.   Click **Yes** at the Confirm UPSR Switch Are You Sure? dialog box.

   i.   Click **OK** at the next dialog box.

Step 2   Check the fiber connections to ensure they are securely fastened and intact.

Step 3   Ensure the OC-N cards are active and in-service.

Step 4   Verify that the protect OC-N card paired with the active reporting OC-N card is the same type and in-service.

Step 5   If the alarm persists and the reporting traffic card is active, do a manual switch to move traffic away from the card:

   a.   At the node view, click the **Maintenance > Protection** tabs.

   b.   Double-click the protection group that contains the reporting card.

   c.   Click the Protect/Standby card of the selected groups.

        d. Click **Manual** and **OK**.

Step 6   Perform a software reset on the reporting card:

        a. Display the CTC node view.

        b. Position the cursor over the slot reporting the alarm.

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

        d. If the alarm persists, physically reseat the reporting card.

Step 7   If the traffic does not switch over, right-click on the protect card and click **Reset**.

Step 8   Attempt another manual switch after the protect cards have booted up completely.

Step 9   If you are still unable to perform a switch, reseat the protect card.

Step 10   Attempt another manual switch.

Step 11   Clear the manual switch:

        a. At the node view, click the **Maintenance > Protection** tabs.

        b. Double-click the protection group that contains the reporting card.

        c. Highlight either selected group.

        d. Click **Clear** and click **YES** at the confirmation dialog box.

Step 12   If the alarm persists, replace the protect card.

> **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   Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.46 FAILTOSWR

- Not Alarmed (NA) (Condition)

This fail to switch ring signals an automatic protection switching (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 an SF or 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 on a Four-Fiber BLSR 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 > Ring** tabs.

   b.   Highlight the row of the affected ring.

   c.   Click **Ring Map**.

   d.   Verify that a Node ID appears in the Ring Map for every node expected to be part of the ring.

Step 2   Display the CTC network view.

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

Step 4   Log into the near-end node and click the **Ring > Provisioning** tabs.

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

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

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

⚠

Caution   Using a test set will disrupt service on the optical card. It may 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.

   Test the line as close to the receiving card as possible.

Step 9   Clean the fiber:

   a.   Clean fiber according to local site practice.

   b.   If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 10   Verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

Step 11   Repeat Steps 1 - 5 for any other ports on the card.

Step 12   Replace the protect standby OC-N card.

Step 13   If the alarm does not clear after you replace the BLSR cards on this node one by one, follow Steps 4 - 14 for each of the nodes in the ring.

Step 14   Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.47 FAILTOSWS

- Not Alarmed (NA) (Condition)

This failure to switch to protection span signals an APS span switch failure. For four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS alarm will 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.

Follow the procedure for .

1.4.48 FAN

- Critical, Service affecting

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 can rise above its normal operating range. The fan tray contains six fans and needs a minimum of five working fans to properly cool the ONS 15454. 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. Plug the wristband cable into the ESD jack located on the lower-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.

Step 2   If the filter is clean, take the fan-tray assembly out of the ONS 15454.

Step 3   Reinsert the fan tray making sure the back of the fan tray connects to the rear of the ONS 15454.

✎

Note   The fan should run immediately when correctly inserted.

Step 4   If the fan does not run or the alarm persists, replace the fan tray.

Step 5   If the replacement fan tray does not operate correctly, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.49 FE-AIS

- Not Alarmed (NA) (Condition)

The far end ais alarm means the far-end node's DS3XM-6 or DS3-12E card is reporting an alarm indication signal (AIS). The prefix FE in an alarm message means the main alarm is occurring at the far-end node and not at the node reporting this FE-AIS alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both the alarms clear when the main alarm clears.

Procedure: Clear the FE-AIS Condition

Step 1   To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 may link to the main AIS alarm from an DS3XM-6 card in Slot 6 of Node 2.

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

Step 3   Clear the main alarm.

1.4.50 FE-DS1-MULTLOS

- Not Alarmed (NA) (Condition)

The far end multiple DS1 LOS detected on DS3XM-6 condition means multiple inputs detect a loss on the far end. The prefix FE in an alarm/condition message means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTOS alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditons clear when the main alarm clears.

Procedure: Clear the FE-DS1-MULTLOS Condition

Step 1   To troubleshoot an FE condition/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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Look up and troubleshoot the main alarm.

1.4.51 FE-DS1-SNGLLOS

- Not Alarmed (NA) (Condition)

The far end single DS1 LOS on the DS3XM-6 condition means one of the DS1-14 inputs on the far end detects an LOS. The prefix FE in an alarm/condition means the main alarm is occurring at the far-end node and not at the node reporting this FE-EQPT-FAILSA alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-SNGLLOS Condition

Step 1   To troubleshoot an FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Look up and troubleshoot the main alarm.

1.4.52 FE-DS3-SA

- Not Alarmed (NA) (Condition)

The far end DS3 equipment failure service affecting alarm means a far-end DS-3 equipment failure is occurring. The prefix FE in an alarm/condition means the main alarm is occurring at the far-end node and not at the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/coditions clear when the main alarm clears.

Procedure: Clear the FE-DS3-SA Condition

Step 1   To troubleshoot an FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Clear the main alarm.

1.4.53 FE-EQPT-NSA

- Not Alarmed (NA) (Condition)

The far end common equipment failure non service affecting condition means a non-service affecting equipment failure is detected in the far-end DS-3. The prefix FE in an alarm/condition message means that the main alarm is occurring at the far-end node, not the node reporting this FE-EQPT-NSA alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

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

Procedure: Clear the FE-EQPT-NSA Condition

Step 1   To troubleshoot an FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Look up and troubleshoot the main alarm.

1.4.54 FE-IDLE

- Not Alarmed (NA) (Condition)

The far end idle condition means a far-end node detects an idle DS-3 signal. The prefix FE in an alarm/condition means that the main alarm is occurring at the far-end node, not the node reporting this FE-IDLE alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Procedure: Clear the FE-IDLE Condition

Step 1   To troubleshoot the FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Clear the main alarm.

1.4.55 FE-LOCKOUT

- Not Alarmed (NA) (Condition)

The far end lockout condition raises whenever the Lockout Protection Span command is entered from any other node. This alarm indicates the prevention of any ring switch requests. The alarm clears when the lock out is removed.

Procedure: Clear the FE-LOCKOUT Condition on a BLSR

Step 1   Display CTC network view.

Step 2   Find the node reporting the LOCKOUT-REQ.

Step 3   Log into the node reporting the LOCKOUT-REQ.

Step 4   Follow the "Clear the Lockout Switch Request and the LOCKOUT-REQ Condition" procedure on page 1-52.

1.4.56 FE-LOF

- Not Alarmed (NA) (Condition)

The far end LOF condition means a far-end node reports a DS-3 loss of frame (LOF). The prefix FE in an alarm/condition means that the main alarm is occurring at the far-end node, not the node reporting this FE-LOF alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-LOF Condition

Step 1   To troubleshoot an FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Look up and troubleshoot the main alarm.

1.4.57 FE-LOS

- Not Alarmed (NA) (Condition)

The far end LOS condition means a far-end node reports a DS-3 loss of signal (LOS). The prefix FE in an alarm/condition message means that the main alarm is occurring at the far-end node, and not at the node reporting this FE-LOS alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-LOS Condition

Step 1   To troubleshoot the FE alarm/condition, 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 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Clear the main alarm.

1.4.58 FEPRLF

- Minor, Non-service affecting

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 occurs on the ONS 15454 when 1+1 bidirectional protection is used on optical cards in a 1+1 configuration.

Procedure: Clear the FEPRLF Alarm on a Four-Fiber BLSR

Step 1   To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.

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

Step 3   Look up and troubleshoot the main alarm.

1.4.59 FORCED-REQ

• Not Alarmed (NA) (Condition)

The force switch request on facility or equipment alarm means a user entered 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 alarm if you want the force switch to remain in place. To clear this alarm, clear the force command.

Procedure: Clear the FORCED-REQ

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**.

1.4.60 FRNGSYNC

• Major, Service affecting

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

Procedure: Clear the FRNGSYNC Alarm

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

Step 2   If the ONS 15454 is configured to operate off 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   Find and troubleshoot alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI and SYNCSEC.

1.4.61 FSTSYNC

• Minor, Non-service affecting

A Fast Start Synchronization mode alarm raises when the ONS 15454 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.

1.4.62 HITEMP

- Critical, Service affecting (NE)
- Minor, Non service affecting (EQPT)

The equipment failure high temperature alarm means the temperature of the ONS 15454 is above 50 degrees Celsius (122 degrees Fahrenheit).

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

Procedure: Clear the HITEMP Alarm

Step 1   Check the temperature of the ONS 15454 on the front panel LCD.

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

Step 3   Ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454.

Step 4   Ensure that blank faceplates fill the ONS 15454 empty slots. Blank faceplates help airflow.

Step 5   Check the condition of the air filter to see if it needs replacement.

Step 6   If the filter is clean, take the fan-tray assembly out of the ONS 15454.

Step 7   Reinsert the fan tray, making sure the back of the fan tray connects to the rear of the ONS 15454.

Note   The fan should run immediately when correctly inserted.

Step 8   If the fan does not run or the alarm persists, replace the fan tray.

Step 9   If the replacement fan tray does not operate correctly, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.63 HLDOVERSYNC

- Major, Service affecting

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

Procedure: Clear the HLDOVERSYNC Alarm

Step 1   Check for additional alarms that relate to timing.

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

1.4.64 IMPROPRMVL

- Critical, Service-affecting

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

Procedure: Clear the IMPROPRMVL Alarm

Step 1   Right-click the card reporting the IMPROPRMVL.

Step 2   Choose **Delete**.

Note   CTC will 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   Before taking the facility out of service, ensure that no live traffic is present on the facility.

    a. In CTC, double-click the reporting card to display the card view.

    b. Click the **Provisioning** tab.

    c. Click the **Status** of any in-service ports.

    d. Choose **Out of Service** to take the ports out of service.

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

⚠

Caution   Before deleting the circuit, ensure that the circuit does not carry live traffic.

    a. At the 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 **SONET DCC > Provisioning** tabs.

    b. Click the slots and ports listed in SDCC Terminations.

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

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

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

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

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

    d. Click **Apply**.

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

1.4.65 INCOMPATIBLE-SW

    • Minor, Non-service affecting

The incompatible software alarm means the CTC software version loaded on the connecting workstation and the CTC software version loaded on the TCC+ card are incompatible. This occurs when the TCC+ software is upgraded but the PC has not yet upgraded the compatible CTC jar file. INCOMPATIBLE-SW also occurs when CTC logs into a node with compatible software but encounters another node in the network that has a newer version of CTC.

Procedure: Clear the INCOMPATIBLE-SW Alarm

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

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser will download the jar file from CTC.

1.4.66 INVMACADDR

• Major, Non-service affecting

The equipment failure invalid MAC address alarm means the ONS 15454 Media Access Control layer address (MAC Address) is invalid. The MAC Address is permanently set into the ONS 15454 chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADDR. Contact the Cisco Technical Assistance Center (TAC) at (1-800-553-2447).

Procedure: Clear the INVMACADDR Alarm

This is not a user-serviceable problem. Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.67 LOCKOUT-REQ

• Not Alarmed (NA) (Condition)

The Lockout Switch Request on Facility/Equipment alarm occurs when a user initiates a lockout switch request for an OC-N card or a lockout switch request on a UPSR at the path level. A lockout prevents protection switching from occurring. Clearing the lockout will again allow protection switching to take place. Clearing the lockout switch request clears the LOCKOUT-REQ alarm. This is an informational alarm.

Procedure: Clear the Lockout Switch Request and the LOCKOUT-REQ Condition

Step 1 Display the CTC network view.

Step 2 Click **Circuits** tab and highlight the circuit.

Step 3 Click **Edit** and click the **UPSR** tab.

Step 4 From the Switch State menu, highlight **Clear**.

Step 5 Click **Apply** and click **Close**.

1.4.68 LOF (BITS)

- Major, Service affecting

The loss of frame alarm means a port on the TCC+ BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data.

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

> ⚠ **Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right 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+:

- **a.** In CTC node view or card view, note the slot and port reporting the alarm.

- **b.** Find the coding and framing formats of the external BITS timing source. 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 screen.

- **d.** Verify that **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 **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 B8ZS coding field is normally paired with ESF in the Framing field, and the AMI coding field is normally paired with SF (D4) in the Framing field.

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC+, replace the TCC+ card.

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

1.4.69 LOF (DS1)

- Major, Service affecting

The loss of frame alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. If the LOF appears on the DS1-14 card, the transmitting equipment may have its framing set to a format that differs from the receiving ONS 15454.

Procedure: Clear the LOF Alarm

Step 1   Verify that the line framing and line coding match between the DS1-14 port and the signal source.

   a. In CTC, note the slot and port reporting the alarm.

   b. Find the coding and framing formats of the signal source for the card reporting the alarm. You may need to contact your network administrator for 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 **Line Type** to reveal a menu. Choose the matching type.

   g. Verify that the reporting Line Coding matches the signal source's Line Type.

   h. If the signal source line coding does not match the reporting port, click **Line Coding** to reveal the menu. Choose the matching type and click **Apply**.

   Note   On the Line tab, the B8ZS coding field is normally paired with ESF in the Framing field. AMI coding is normally paired with SF (D4) in the Framing field.

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

1.4.70 LOF (DS3)

   • Critical, Service affecting

The loss of frame alarm indicates that the receiving ONS 15454 lost frame delineation in the incoming data. The framing of the transmitting equipment may be set to a format that differs from the receiving ONS 15454. On DS3-12E cards, the alarm occurs only on cards with the provisionable framing format set to C-bit or M23, not on cards with the provisionable framing format is set to unframed.

Procedure: Clear the LOF Alarm

Step 1   Change the line type of the non-ONS equipment attached to the reporting card to C-bit.

1.4.71 LOF (EC1-12)

- Critical, Service affecting

The loss of frame alarm means a port on the reporting EC1-12 card has a LOF condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

LOF on an EC1-12 card is sometimes an indication that the EC1-12 card reporting the alarm expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

⚠️

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

Procedure: Clear the LOF Alarm

Step 1 The LOF should trigger an automatic protection switch away from the working card that reported the alarm. If it did not, do a manual switch to move traffic away from the reporting card:

   a. At the node view, click the **Maintenance > Protection** tabs.

   b. Double-click the protection group that contains the reporting card.

   c. Click the Protect/Standby card of the selected groups.

   d. Click **Manual** and **OK**.

Step 2 Clear the manual switch:

   a. At the node view, click the **Maintenance >Protection** tabs.

   b. Double-click the protection group that contains the reporting card.

   c. Highlight either selected group.

   d. Click **Clear** and click **YES** at the confirmation dialog box.

   ✎

   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 3 If you still receive the LOF alarm, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.72 LOF (OC-N)

- Critical, Service affecting

The loss of frame alarm means a port on the reporting OC-N card has an LOF condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

LOF on an OC-N card is sometimes an indication that the OC-N card reporting the alarm expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

⚠

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

Procedure: Clear the LOF Alarm

Step 1   The LOF should trigger an automatic protection switch away from the working card that reported the alarm. If it did not, do a manual switch to move traffic away from the reporting card:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Click the Protect/Standby card of the selected groups.

    d. Click **Manual** and **OK**.

✎

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 2   Clear the manual switch:

    a. At the node view, click the **Maintenance > Protection** tabs.

    b. Double-click the protection group that contains the reporting card.

    c. Highlight either selected group.

    d. Click **Clear** and click **YES** at the confirmation dialog box.

Step 3   Verify that the OC-N port on the upstream node is in-service.

Step 4   If you continue to receive the LOF alarm, see the "Faulty Fiber-Optic Connections" section on page 2-38.

1.4.73 LOGBUFR90

- • Major, Service affecting

The log buffer 90% full alarm means that the memory buffer holding the alarms seen on the Alarms pane in CTC is 90% full. If the buffer continues to fill, a LOGBUFROVFL alarm is reported. The LOGBUFROVFL alarm means the memory buffer is full, and any new alarms occurring on the ONS 15454 will not display on the CTC alarms pane. The CTC receives alarms from all ONS nodes on the network, even if the CTC is set to the node or card level view.

Procedure: Clear the LOGBUFR90 Alarm

Step 1   Click the close button on the upper right corner of the CTC screen.

Step 2   Click the close button on the upper right corner of the browser screen.

Step 3   Log back into the ONS 15454. The LOGBUFR90 alarm should clear after an approximately one minute delay.

Exiting CTC and logging back into the ONS 15454 removes any cleared alarms from the log buffer and resynchronizes the alarm pane to show any alarms that were not displayed as a result of a full log buffer.

Note   Checking the AutoDelete Cleared Alarms checkbox on the Alarms panel helps prevent log buffer overflow.

1.4.74 LOGBUFROVFL

- Major, Service affecting

The log buffer overflow alarm means the memory buffer is full, and any new alarms occurring on the ONS 15454 will not display on the CTC alarms pane. The CTC receives alarms from all ONS nodes on the network, even if the CTC is set to the node or card level view.

Procedure: Clear the LOGBUFROVFL Alarm

Step 1   Click the close button on the upper right corner of the CTC screen.

Step 2   Click the close button on the upper right corner of the browser screen.

Step 3   Log back into the ONS 15454. The LOGBUFROVFL alarm should clear after an approximately one minute delay.

Exiting CTC and logging back into the ONS 15454 removes any cleared alarms from the log buffer and resynchronizes the alarm pane to show any alarms not displayed as a result of a full log buffer.

Note   Checking the AutoDelete Cleared Alarms checkbox on the Alarms panel helps prevent log buffer overflow.

1.4.75 LOP-P

- Critical, Service affecting

This loss of pointer path alarm indicates a loss of pointer (LOP) at the path level. LOP occurs when valid H1/H2 pointer bytes are missing from the SONET overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. A LOP alarm means that eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

One of the conditions that can cause this alarm is a transmitted STSc circuit that is smaller than the provisioned STSc. This condition causes a mismatch of the circuit type on the concatenation facility. For example, if an STS-3c or STS-1 is sent across a circuit provisioned for STS-12c, a LOP alarm occurs.

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

Procedure: Clear the LOP-P Alarm

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

Step 2   Perform a soft reset on the reporting card:

   a. Display the CTC node view.

   b. Position the cursor over the slot reporting the alarm.

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

Step 3   Do a manual switch (side switch) to move traffic away from the card.

   a. At the node view, click the **Maintenance > Protection** tabs.

   b. Double-click the protection group that contains the reporting card.

   c. Click the Protect/Standby card of the selected groups.

   d. Click **Manual** and **OK**.

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:

   a. At the node view, click the **Maintenance > Protection** tabs.

   b. Double-click the protection group that contains the reporting card.

   c. Highlight either selected group.

   d. Click **Clear** and click **YES** at the confirmation dialog box.

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   Do a soft reset on the far-end card:

   a. Display the CTC node view.

   b. Position the cursor over the slot reporting the alarm.

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

Step 7   Perform a soft reset on the reporting card:

      a. Display the CTC node view.

      b. Position the cursor over the slot reporting the alarm.

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

Step 8   Switch from the far-end working card to the far-end protect card.

Step 9   If the alarm persists, replace the far-end card.

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

1.4.76 LOP-V

- Major, Service affecting

The loss of pointer VT alarm indicates a loss of pointer at the VT level. The VT, or electrical, layer occurs when the SONET signal is broken down into an electrical signal, for example, when an optical signal comes into an ONS 15454. The ONS 15454 demultiplexes this optical signal. One of the channels separated from the optical signal cross connects into a ONS 15454 DS3XM-6 or DS1-14 port. The ONS 15454 reports the LOS-V alarm.

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

Procedure: Clear the LOP-V Alarm

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

Step 2   Perform a software reset on the reporting card:

      a. Display the CTC node view.

      b. Position the cursor over the slot reporting the alarm.

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

Step 3   Do a manual switch to move traffic away from the card:

      a. At the node view, click the **Maintenance > Protection** tabs.

      b. Double-click the protection group that contains the reporting card.

      c. Click the Protect/Standby card of the selected groups.

      d. Click **Manual** and **OK**.

> **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:

   a.   At the node view, click the **Maintenance > Protection** tabs.

   b.   Double-click the protection group that contains the reporting card.

   c.   Highlight either selected group.

   d.   Click **Clear** and click **YES** at the confirmation dialog box.

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

Step 6   Do a soft reset on the far-end card.

Step 7   Switch from the far-end working card to the far-end protect card.

1.4.77 LOS (BITS)

   • Major, Service affecting

The TCC+ card has a loss of signal (LOS) from the BITS timing source. An LOS occurs when a SONET 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. 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 backplane BITS clock pin fields to the timing source.

Step 2   Check that the BITS clock is operating properly.

1.4.78 LOS (DS-N)

   • Critical, Service affecting

This alarm indicates a loss of signal (LOS) at the card for either a DS-3 port or a DS1-14 port. LOS 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. 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 cabling continuity to the port.

Step 2   Verify that the correct port is in-service.

Step 3   Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible.

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.

Step 6   Repeat Steps 1 - 5 for another port on the card.

Step 7   Look for another alarm that may identify the source of the problem.

Step 8   Replace the reporting card.

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

1.4.79 LOS (EC1-12)

- Critical, Service affecting

A port on the reporting EC1-12 card has a loss of signal (LOS) condition. An LOS occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS means the upstream transmitter has failed. If an EC1-12 LOS alarm is not accompanied by additional alarms, a fiber break or cabling problem is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.

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

Procedure: Clear the LOS Alarm

Step 1   Verify cabling continuity to the port.

Step 2   Verify that the correct port is in-service.

Step 3   Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible.

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 cable connector on the ONS 15454.

Step 6   Repeat Steps 1 - 5 for another port on the card.

Step 7   Look for another alarm that may identify the source of the problem.

Step 8   Replace the reporting card.

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

1.4.80 LOS (OC-N)

- Critical, Service affecting

A port on the reporting OC-N card has a loss of signal (LOS) condition. An LOS occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.

> ⚠
> **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.**

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

Procedure: Clear the LOS Alarm

Step 1   Verify fiber continuity to the port.

Step 2   Verify that the correct port is in-service.

Step 3   Use an optical test set to verify that a valid signal exists on the line.

Test the line as close to the receiving card as possible.

Step 4   Clean the fiber:

    a.   Clean fiber according to local site practice.

    b.   If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 5   Verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications for each card.

Step 6   If there is a valid signal, replace the connector on the backplane.

Step 7   Repeat Steps 1 - 5 for another port on the card.

Step 8   Replace the OC-N card.

1.4.81 LPBKDS1FEAC

- Not Alarmed (NA) (Condition)

A loopback due to FEAC command DS1 condition on the DS3XM-6 card means a DS-1 loopback signal is received from the far-end node due to a Far-End Alarm and Control (FEAC) command. An FEAC command is often used with loopbacks.

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 about loopbacks, see the "Network Troubleshooting Tests" section on page 2-1.

⚠

Caution   The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

✎

Note   This is an informational alarm.

1.4.82 LPBKDS3FEAC

- Not Alarmed (NA) (Condition)

A loopback due to FEAC command DS3 condition means a DS-3 loopback signal is received from the far-end node because of a Far-End Alarm and Control (FEAC) command. An FEAC command is often used with loopbacks. This condition is only reported by DS3-12E or DS3XM-6 cards. A DS3XM-6 card both generates and reports FEAC alarm/conditions, but a DS3-12E card only reports FEAC alarms/conditions.

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 about loopbacks, see the "Network Troubleshooting Tests" section on page 2-1.

⚠

Caution   The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

✎

Note   This is an informational alarm.

1.4.83 LPBKFACILITY (DS-N or EC1-12)

- Not Alarmed (NA) (Condition)

A loopback facility alarm means 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 "Network Troubleshooting Tests" section on page 2-1.

There are two types of loopbacks: 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.

✎ **Note**   DS3XM-6 cards only support facility loopbacks on DS-1 circuits.

Procedure: Clear the LBKFACILITY Condition

Step 1   Double-click the reporting card in CTC or right-click the reporting card in CTC and choose **Open** from the menu.

Step 2   Click the **Maintenance** tab.

    a. If the condition is reported against a DS3XM-6 card, also click the **DS1** tab.

    b. If a Loopback Type column cell that displays Facility (Line) is not shown under the **DS1** tab, then click the **DS3** tab to reveal a Loopback Type column cell that displays Facility (Line).

Step 3   Click the Loopback Type column cell that displays Facility (Line).

Step 4   Click **None**, and click **Apply**.

1.4.84 LPBKFACILITY (OC-N)

    • Not Alarmed (NA) (Condition)

A loopback facility alarm means 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 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.

⚠️

Caution   Before performing a facility loopback on an OC-N card, make sure there is another SDCC path to the ONS 15454 containing the OC-N card being put in loopback. A second SDCC path is necessary so you have a non-looped back path to log into the ONS 15454 containing the OC-N card being put in loopback and remove the facility loopback. This is not necessary if you are directly connected to the ONS 15454 with the OC-N card in facility loopback.

Procedure: Clear the LBKFACILITY Condition

Step 1   To remove the loopback alarm, double-click or right-click on the reporting card in the CTC. Choose **Open** from the list of options.

Step 2   Click the **Maintenance** tab.

Step 3   Click the Loopback Type column and choose **None** from the menu.

Step 4   Click **Apply**.

1.4.85 LPBKTERMINAL (DS-N, EC1-12)

- Not Alarmed (NA) (Condition)

A loopback terminal alarm means 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.

✎

Note   Terminal loopback is not supported at the DS1 level for the DS3XM-6 card.

Procedure: Clear the LBKTERMINAL Condition

Step 1   To remove the loopback alarm, double-click or right-click on the reporting card in the CTC. Choose **Open** from the list of options.

Step 2   Click the **Maintenance** tab.

Step 3   Click the Loopback Type column and choose **None** from the menu.

Step 4   Click **Apply**.

1.4.86 LPBKTERMINAL (G1000-4)

- Not Alarmed (NA) (Condition)

A loopback terminal alarm means 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.

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. G1000-4 cards only support Terminal loopbacks. 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.

Procedure: Clear the LPBKTERMINAL Condition

Step 1 To remove the loopback alarm, double-click the reporting card in CTC, or right-click the reporting card and choose **Open** from the list of options.

Step 2 Click the **Maintenance** tab.

Step 3 Choose the Loopback Type column and choose **None** from the menu.

Step 4 Click **Apply**.

1.4.87 LPBKTERMINAL (OC-N)

- Not Alarmed (NA) (Condition)

A loopback terminal alarm means 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 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 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 LBKTERMINAL Condition

Step 1 To remove the loopback alarm, double-click or right-click on the reporting card in the CTC. Choose **Open** from the list of options.

Step 2 Click the **Maintenance** tab.

Step 3 Click the Loopback Type column and choose **None** from the menu.

Step 4   Click **Apply**.

1.4.88 MAN-REQ

- Not Alarmed (NA) (Condition)

The Manual Switch Request on a Facility/Equipment alarm occurs when a user initiates a manual switch request on an OC-N card or UPSR path. Clearing the manual switch clears the MANUAL-REQ alarm.

Procedure: Clear the Manual Switch and the MAN-REQ Condition

Step 1   From network view, click the **Circuits** tab.

Step 2   Highlight the circuit.

Step 3   Click **Edit** and click the **UPSR** tab.

Step 4   From the Switch State menu, highlight **Clear**.

Step 5   Click **Apply** and click **Close**.

1.4.89 MANRESET

- Not Alarmed (NA) (Condition)

A maual system reset condition means a user performed a manual system reset by right-clicking a card and chose **Reset**. Resets performed during a software upgrade also prompt the alarm. This condition clears automatically, when the card finishes resetting.

1.4.90 MEA (AIP)

- Critical, Service affecting

If the mismatch between entity/equipment type and provisioned attributes alarm is reported against the Alarm Interface Panel (AIP), the fuse in the AIP board blew or is missing. This alarm also occurs when an old AIP board with a 2 amp fuse is installed in a newer 10 Gbps compatible or ANSI shelf assembly (15454-SA-ANSI). In either case, replace the AIP.

Procedure: Clear the MEA Alarm

Follow the "Alarm Interface Panel Replacement" section on page 3-7.

1.4.91 MEA (EQPT)

- Critical, Service affecting

The mismatch between entity/equipment type and provisioned attributes alarm is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or laterare inserted into an older, pre-ANSI (15454-SA-NEBS3E or older) shelf assembly or older Ethernet cards (E1000-2 and E100T-12) are used in a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI). Removing the incompatible cards to clear the alarm.

Procedure: Clear the MEA Alarm

Step 1   Determine whether the ONS 15454 shelf assembly is a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) or an earlier shelf assembly. At the CTC shelf view, click the **Inventory** tab.

Under the Hardware Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf or 10 Gbps compatible shelf assembly.

Under the Hardware Part # column, if the number is not 800-19856-XX or 800-19856-XX, then you are using an earlier shelf assembly.

> ✎
> **Note**   On the 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 2   Physically verify the type of card that sits in the slot reported in the object column of the MEA row on the alarms screen by reading the name at the top of the card's faceplate.

a.   If you have a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 3.

b.   If you have a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed.

> ✎
> **Note**   The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10 Gbps compatible shelf assembly and are the functional equivalent of the older, 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 ANSI 10 Gbps compatible shelf assembly.

c.   If you have an older, pre-ANSI 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-ANSI 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 any slot (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).

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 turned on, or is used as a timing reference, then CTC will 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 **Status** of any in-service ports.

    d.   Choose **Out of Service** to take the ports out of service.

Step 7   If a circuit has been mapped to the card, delete the circuit:

> ⚠
> **Caution**   Before deleting the circuit, ensure that no live traffic exists on the facility.

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

    b.   Choose the applicable circuit (the one that connects to the reporting card).

    c.   Click **Delete**.

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.

1.4.92 MEA (FAN)

- Critical, Service affecting

The mismatch between entity/equipment type and provisioned attributes alarm is reported against the fan tray when a newer fan-tray assembly (15454-FTA3) with a 5 amp fuse is used with an older shelf assembly or when an older fan tray with a 2 amp fuse is used with a newer 10 Gbps compatible or ANSI shelf assembly (15454-SA-ANSI) that contains cards introduced in Release 3.1 or later. If a newer ANSI shelf assembly contains only cards introduced before Release 3.1, then an older fan tray assembly (15454-FTA-2) can be used and will not report an MEA alarm.

Procedure: Clear the MEA Alarm

Step 1   Determine whether the ONS 15454 shelf assembly is a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) or an earlier shelf assembly. At the CTC shelf view, click the **Inventory** tab.

Under the Hardware Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf or 10 Gbps compatible shelf assembly.

Under the Hardware Part # column, if the number is not 800-19857-XX or 800-19856-XX, then you are using an earlier shelf assembly.

Step 2   If you have a 15454-SA-ANSI shelf or 10 Gbps compatible shelf assembly, the alarm indicates that an older incompatible fan tray assembly is installed in the shelf assembly. See the "Fan-Tray Assembly Replacement" section on page 3-5.

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 see the "Fan-Tray Assembly Replacement" section on page 3-5.

1.4.93 MEM-GONE

- Major, Non-service affecting

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC+ card. CTC will not function properly until this alarm clears. The alarm clears when additional memory becomes available.

Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.94 MEM-LOW

- Minor, Non-service affecting

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+ card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC+ card is exceeded, CTC will cease to function.

Log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.95 MFGMEM

- Critical, Service Affecting

The MFGMEM or Manufacturing Data Memory Failure alarm raises if the ONS 15454 cannot access the data in the erasable programmable read-only memory (EPROM). Either the memory module on the component failed or the TCC+ lost the ability to read that module. The EPROM stores manufacturing

data that is needed for both compatibility and inventory issues. The EPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address will disrupt IP connectivity and gray out the ONS 15454 icon on the CTC network view.

Procedure: Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane.

Step 1   Do a software-initiated system reset on the TCC+ by referring to the "Perform a Software-Initiated Reset" procedure on page 3-14.

Step 2   If the alarm does not clear, do a card pull reset on the TCC+ by referring to the "Perform a Card Pull" procedure on page 3-14.

Step 3   If the alarm does not clear, physically replace the standby TCC+ card on the ONS 15454 with a new TCC+ card.

    a.   Open the TCC+ card ejectors.

    b.   Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.

    c.   Open the ejectors on the TCC+ card.

    d.   Slide the TCC+ card into the slot along the guide rails.

    e.   Close the ejectors.

Note   It takes approximately 20 minutes for the active TCC+ to transfer the system software to the newly-installed TCC+. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the LEDs on the TCC+ flash Fail and then the Active/Standby LED flashes. When the transfer completes, the TCC+ reboots and goes into Standby mode after approximately three minutes.

Step 4   Right click the active TCC+ card to reveal a pull-down menu.

Step 5   Click **Reset Card**.

Wait for the TCC+ to reboot. The ONS 15454 switches the standby TCC+ card to active mode.

Step 6   Verify that the remaining TCC+ card is now in standby mode (the ACT/STBY LED changes to amber).

Step 7   Physically replace the remaining TCC+ card with the second TCC+ card.

    a.   Open the TCC+ card ejectors.

    b.   Slide the card out of the slot.

    c.   Open the ejectors on the TCC+ card.

    d.   Slide the TCC+ card into the slot along the guide rails.

    e.   Close the ejectors.

The ONS 15454 boots up the second TCC+ card. The second TCC+ must also copy the system software, which can take up to twenty minutes.

Step 8   If the MFGMEM alarm continues to report after replacing the TCC+ cards, the problem lies in the EPROM.

Step 9   If the MFGMEM is reported from the fan tray, replace the fan tray.

Step 10   If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan tray is replaced, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

1.4.96 NOT-AUTHENTICATED

• Minor, Non-service affecting

This not authenticated alarm indicates that the username and password entered do not match the information stored in the TCC+. 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.

Note   For initial log on to the ONS 15454, type the user name CISCO15 and click **Login** (no password is required).

Procedure: Clear the NOT-AUTHENTICATED Alarm

Step 1   If you have an alternate username and a password available to access the system:

a.   Use the alternate username and password to access the ONS node.

b.   Click the **Provisioning > Security** tabs.

c.   Look under the Users field to find the username that raised the alarm.

d.   If the username that raised the alarm is listed, then highlight the username to reveal the associated password. Record the correct password.

e.   If the username is not listed, then click **Create**.

f.   Fill in the fields on the Create User dialog box with the username and password that raised the alarm then click **OK**.

Step 2   If you do not have an alternate username and password available, call the Cisco Technical Assistance Center at (1-800-553-2447). TAC can issue a new username and password.

1.4.97 PDI-P

• Not Alarmed (NA) (Condition)

A Payload Defect Indication Path alarm indicates a signal label mismatch failure (SLMF). An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal label byte. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15454 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS alarm often accompanies the PDI-P alarm. If the PDI-P is the only alarm reported with the AIS, clear the PDI-P alarm to clear the AIS alarm. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid alarm.

A PDI-P condition reported on the port of an OC-N card supporting a G1000-4 card circuit may result from the end-to-end Ethernet link integrity feature of the G1000-4. This will typically be accompanied by an alarm, such as TPTFAIL or CARLOSS, reported against one or both Ethernet ports terminating the circuit. In this instance troubleshooting the accompanying alarm will clear the PDI-P condition.

⚠

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.**

⚠

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

Procedure: Clear the PDI-P Condition

Step 1 Verify that all circuits terminating in the reporting card are in an active state:

   a. 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, wait 10 minutes for the ONS 15454 to fully initialize. If INCOMPLETE does not change after full initialization, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 2 After determining that the port is active, verify the signal source to the card reporting the alarm.

Step 3 If traffic is affected, delete and recreate the circuit.

⚠

Caution Deleting a circuit may affect traffic.

Step 4 Check the far-end OC-N card that provides STS payload to the reporting card.

Step 5 Confirm the cross-connect between the OC-N card and the reporting card.

Step 6 Clean the far-end optical fiber:

   a. Clean the fiber according to local site practice.

   b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 7 Replace the optical/electrical cards.

✎

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

1.4.98 PEER-NORESPONSE

- Major, Non-service affecting

The switch agent raises a peer card not responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. This is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Procedure: Clear the PEER-NORESPONSE Alarm Reported

Step 1   Right click on the card reporting the alarm.

Step 2   Click **Reset Card** and **OK** on the confirmation dialog.

Step 3   Wait for the card to reset.

Step 4   At reset, the green Act LED on the card will be replaced on the CTC by a white Ldg LED. When the card finishes resetting, the green Act LED will reappear.

Step 5   Right click on the peer card of the card reporting the alarm.

Step 6   Click **Reset Card** and **OK** on the confirmation dialog.

1.4.99 PLM-P

- Critical, Service affecting

A Payload Label Mismatch Path indicates a Signal Label Mismatch Failure (SLMF). An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal label byte. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15454 encounters an SLMF when the payload, such as a DS-3 signal, does not match what the signal label is reporting. An AIS alarm often accompanies the PLM-P alarm. If the PLM-P is the only alarm reported with the AIS, clearing the PLM-P alarm clears the AIS alarm.

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.**

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

Procedure: Clear the PLM-P Alarm

Step 1   Verify that all circuits terminating in the reporting card are active:

a.   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, wait 10 minutes for the ONS 15454 to fully initialize. If INCOMPLETE does not change after full initialization, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 2   After determining the port is active, verify the signal source to the traffic card reporting the alarm.

Step 3   If traffic is being affected, delete and recreate the circuit.

⚠

Caution   Deleting a circuit may affect traffic.

Step 4   Check the far-end OC-N card that provides STS payload to the DS-N card.

Step 5   Verify the cross-connect between the OC-N card and the DS-N card.

Step 6   Clean the far-end optical fiber:

   a.   Clean the fiber according to local site practice.

   b.   If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 7   Replace the OC-N/DS-N cards.

✎

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

1.4.100 PLM-V

- Minor, Service affecting

A VT Payload Label Mismatch alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. This alarm occurs when ONS nodes interoperate with equipment that performs bit-synchronous mapping for DS-1. ONS nodes use asynchronous mapping.

Procedure: Clear the PLM-V Alarm

Step 1   Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.

Step 2   Verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

1.4.101 PRC-DUPID

- Major, Service affecting

The procedural error duplicate node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Procedure: Clear the PRC-DUPID Alarm

Step 1 Find the nodes with identical node IDs.

    a. Log into a node on the ring.

    b. Click the **Provisioning > Ring** tabs.

    c. Record the Node ID number.

    d. Repeat steps a – c for all nodes in the ring.

Step 2 If two nodes have an identical node ID number, change the node ID number of one node.

    a. Log into a node that has an identical node ID number.

    b. Click the **Provisioning > Ring** tabs.

    c. Change the number in the Node ID field to a unique number between 0 and 31.

    d. Click **Apply**.

1.4.102 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 SONET path to the other.

RAI on the DS3XM-6 card indicates that far-end node is receiving a DS-3 AIS.

Procedure: Clear the RAI Condition

Use the AIS procedure to troubleshoot the far-end DS-3 node for RAI.

1.4.103 RCVR-MISS

- Major, Service affecting

A facility termination equipment receiver missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. This usually occurs when a missing receive cable on the DS1-14 port or a possible mismatch of backplane equipment, for example, an SMB connector or a BNC connector is connected to a DS1-14 card.

Note DS-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

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

Procedure: Clear the RCVR-MISS Alarm

Step 1   Ensure that the device attached to the DS1-14 port is operational.

Step 2   Verify that the cabling is securely connected.

Step 3   Verify that the pinouts are correct.

Step 4   Replace the receive cable if Steps 1 – 3 do not clear the alarm.

1.4.104 RDI-P

See the .

1.4.105 RFI-L

- Not reported

A Remote Fault Indication alarm occurs when the ONS 15454 detects a remote fault indication (RFI) in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L alarm in the reporting node.

RFI-L indicates that the alarm is occurring at the line level. The line layer is the segment between two SONET devices in the circuit and is also known as a maintenance span. The line layer deals with SONET payload transport. The line layer functions include multiplexing and synchronization.

Procedure: Clear the RFI-L Condition

Step 1   Log into the far-end node from the reporting ONS 15454.

Step 2   Check for alarms in the far-end node, especially LOS.

Step 3   Resolve alarms in the far-end node.

1.4.106 RFI-P

- Not reported

A Remote Failure Indication Path alarm occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P alarm in the reporting node.

RFI-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment may encompass several consecutive line segments. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15454, often perform the origination and termination tasks of the SONET payload.

An RFI-P error message on the ONS 15454 indicates that the node reporting the RFI-P is the terminating node on that path segment.

Cisco ONS 15454 Troubleshooting and Maintenance Guide, R3.2

Procedure: Clear the RFI-P Condition

Step 1   Verify that the ports are enabled and in-service on the reporting ONS 15454.

Step 2   To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3   Check for alarms in the node with the failure, especially UNEQ-P or UNEQ-V.

Step 4   Resolve alarms in that node.

1.4.107 RFI-V

- Not reported

A Remote Fault Indication VT alarm occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V alarm in the reporting node.

RFI-V indicates that an upstream failure has occurred at the VT layer. The VT (electrical) layer is created when the SONET signal is broken down into an electrical signal, for example when an optical signal comes into an ONS 15454. If this optical signal is demultiplexed and one of the channels separated from the optical signal is cross connected into the DS1-14 port in the ONS 15454, the ONS 15454 reports an RFI-V alarm.

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

Procedure: Clear the RFI-V Condition

Step 1   Check connectors to ensure they are securely fastened and connected to the correct slot/port.

Step 2   Verify that the DS1-14 port is active and in-service.

Step 3   Check the signal source for errors.

Step 4   Log into the far-end node from the reporting ONS 15454.

Step 5   Check for alarms in the far-end node, especially UNEQ-P or UNEQ-V.

Step 6   Find and troubleshoot the far-end node alarms.

1.4.108 RING-MISMATCH

- Major, Service affecting

A procedural error mismatch ring alarm occurs when the Ring ID of the ONS 15454 that is reporting the alarm does not match the Ring ID of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical Ring IDs to function.

Procedure: Clear the RING-MISMATCH Alarm

Step 1   Click the **Provisioning > Ring** tabs.

Step 2   Note the number in the Ring ID field.

Step 3   Log into the next ONS node in the BLSR.

Step 4   Verify that the Ring ID number matches the Ring ID number of the reporting node.

    a.   If the Ring ID matches the Ring ID in the reporting ONS node, log into the next ONS node in the BLSR.

    b.   If the Ring ID does not match the Ring ID in the reporting ONS node, change the Ring ID to match the Ring ID of the reporting node and click **Apply**.

    c.   Click **Yes** on the Accept Ring Map Changes dialog box.

    d.   Verify that the ring map is correct.

    e.   Click **Accept** for the new BLSR Ring Map.

Step 5   Repeat Step 4 for all ONS nodes in the BLSR.

1.4.109 SD-L

- Not Alarmed (NA) (Condition)

A signal degrade alarm occurs when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the signal degrade (SD) threshold. Signal degrade is defined by Telcordia as a "soft failure" condition. SD and signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

The BER threshold on the ONS 15454 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}.

SD-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SD alarm travels on the B2 byte of the SONET overhead.

The SD 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.

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.**

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

Procedure: Clear the SD-L Condition

Step 1   Verify that the user-provisonable BER threshold is set at the expected level.

    a.   From the CTC node view, double-click the card reporting the alarm to bring up the card view.

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

    c. Under the SD BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.

    d. If the entry is consistent with what the system was originally provisioned for, continue to step 2.

    e. If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.

    f. Click **Apply**.

Step 2 With an optical test set, measure the power level of the line to ensure it is within guidelines.

Step 3 Verify that optical receive levels are within the acceptable range.

Step 4 Clean the fibers at both ends for a line signal degrade:

    a. Clean the fiber according to local site practice.

    b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

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 may be failing and require replacement.

1.4.110 SD-P

- Not Alarmed (NA) (Condition)

A signal degrade alarm occurs when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the signal degrade (SD) threshold. Signal degrade is defined by Telcordia as a "soft failure" condition. SD and signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF. SD causes the card to switch from working to protect.

The BER threshold on the ONS 15454 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}.

SD-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SD alarm travels on the B3 byte of the SONET overhead. The ONS 15454 detects path SD on the STS level, not the VT level.

The SD 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.

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.**

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

Procedure: Clear the SD-P Condition

Step 1   Verify that the user-provisonable BER threshold is set at the expected level.

  a. From the CTC node view, double-click the card reporting the alarm to bring up the card view.

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

  c. Under the SD BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.

  d. If the entry is consistent with what the system was originally provisioned for, continue to step 2.

  e. If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.

  f. Click **Apply**.

Step 2   With an optical test set, measure the power level of the line to ensure it is within guidelines.

Step 3   Verify that optical receive levels are within the acceptable range.

Step 4   Verify that single-mode fiber is being used.

Step 5   Verify that a single-mode laser is being used at the far end.

Step 6   If the problem persists, the transmitter at the other end of the optical line may be failing and require replacement.

1.4.111 SF-L

- Not Alarmed (NA) (Condition)

A signal failure alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. . 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.

The BER threshold on the ONS 15454 is user provisionable and has a range for SF from 10^{-5} to 10^{-3}.

SF-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SF alarm travels on the B2 byte of the SONET overhead.

SF causes a card to switch from working to protect at either the path or line 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.

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.**

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

Procedure: Clear the SF-L Condition

Step 1 Verify that the user-provisonable BER threshold is set at the expected level.

    a. From the CTC node view, double-click the card reporting the alarm to bring up the card view.

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

    c. Under the SF BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.

    d. If the entry is consistent with what the system was originally provisioned for, continue to step 2.

    e. If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.

    f. Click **Apply**.

Step 2 Using an optical test set, measure the power level of the line and ensure it is within the guidelines.

Step 3 Verify that optical receive levels are within the acceptable range.

Step 4 Clean the fibers at both ends for a line signal fail:

    a. Clean the fiber according to local site practice.

    b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

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 may be failing and need replacement.

1.4.112 SF-P

• Not Alarmed (NA) (Condition)

A signal failure alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. 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.

The BER threshold on the ONS 15454 is user provisionable and has a range for SF from 10^{-5} to 10^{-3}.

SF-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SF alarm travels on the B3 byte of the SONET overhead. The ONS 15454 detects path SF on the STS level, not the VT 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.

⚠

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.**

⚠

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

Procedure: Clear the SF-P Condition

Step 1   Verify that the user-provisonable BER threshold is set at the expected level.

    a.   From the CTC node view, double-click the card reporting the alarm to bring up the card view.

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

    c.   Under the SF BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.

    d.   If the entry is consistent with what the system was originally provisioned for, continue to step 2.

    e.   If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.

    f.   Click **Apply**.

Step 2   Using an optical test set, measure the power level of the line and ensure it is within the guidelines.

Step 3   Verify that optical receive levels are within the acceptable range.

Step 4   Verify that single-mode fiber is being used.

Step 5   Verify that a single-mode laser is being used at the far-end node.

Step 6   If the problem persists, the transmitter at the other end of the optical line may be failing and need replacement.

1.4.113 SFTWDOWN

- Minor, Non-service affecting

A software download in progress alarm occurs, when the TCC+ is downloading or transferring software. No action is necessary. Wait for the transfer or the software download to complete.

1.4.114 SFTWDOWN-FAIL

- Minor, Non-service affecting

The software download from the TCC+ card to the ONS 15454 failed. The problem lies in the TCC+ card.

Procedure: Clear the SFTWDOWN-FAIL Alarm

Step 1   Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.

Step 2   If the download fails, reset the standby TCC+ to ensure that the standby card is synchronized with the database on the active TCC+:

    a.   Identify the standby TCC+.

        If you are looking at the physical ONS 15454, the ACT/STBY LED of standby TCC+ is amber .

        If you are looking at the CTC node view of the ONS 15454, the standby TCC+ has a yellow LED depiction with the letters "Sby".

    b.   Right-click on the standby TCC+.

    c.   Select **Reset Card** from the pull-down menu.

    d.   Click **Yes** at the Are You Sure dialog that appears.

        While the card resets, the FAIl LED will blink on the physical card and then no LED will be lit.

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

    e.   Verify that the reset is complete and error free.

        No new alarms appear under the alarms tab on the CTC.

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

        If you are looking at the CTC node view of the ONS 15454, a yellow LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

    f.   Wait ten minutes to verify that the Standby TCC+ does not reset itself.

    g.   If the TCC+ reset is not complete and error free or if the TCC resets itself, call the Cisco Technical Assistance Center (1-800-553-2447).

Step 3   Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.

Step 4   If the software download fails again, refer to and complete the Back Up and Restore the Database procedure in the ONS 15454 Procedure Guide, then proceed to the next step in this procedure.

Step 5   Reset the active TCC+:

    a.   Identify the active TCC+.

        If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+ is green.

        If you are looking at the CTC node view of the ONS 15454, the active TCC+ has a green LED depiction with "Act".

    b.   Right-click on the active TCC+.

    c.   Select **Reset Card** from the pull-down menu.

    d.   Click **Yes** at the Are You Sure dialog that appears.

    e.   Wait ten minutes to verify that the newly standby TCC+ does not reset itself.

    f.   Verify that the reset is complete and error free.

        No new alarms appear under the alarms tab on the CTC.

        If you are looking at the physical ONS 15454, the ACT/STBY LED has stopped blinking and is now amber.

        If you are looking at the CTC node view of the ONS 15454, a yellow LED depiction with Sby has replaced the blue/white depiction on the card in CTC. (The formerly active TCC+ is now standby.)

    g.   If the TCC+ reset is not complete and error free or if the TCC resets itself, call the Cisco Technical Assistance Center (1-800-553-2447).

Step 6   Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.

Step 7   If the download fails again, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

1.4.115 SQUELCH

- Not Alarmed, Non-service affecting (Condition)

The ring is squelching traffic alarm occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenanceforce ring commands. The isolation or failure of the node will disable 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 AIS-P alarm will also appear 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

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.**

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 grayed out node with red spans will be 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.

Step 4   Use an optical test set to verify that a valid signal exists on the line.

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. Each individual card section in Chapter 4 lists the receiver specifications for that card.

Step 6   Ensure that the optical transmits and receives are connected properly.

Step 7   Replace the OC-N card.

1.4.116 SSM-FAIL

- Minor, Non-service affecting

The failed to receive synchronization status message alarm means the synchronization status messaging (SSM) received by the ONS 15454 failed. The problem is external to ONS 15454. The ONS 15454 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

SSM is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET line layer. They enable SONET devices to automatically select the highest quality timing reference and to avoid timing loops.

Procedure: Clear the SSM-FAIL Alarm

Step 1   Check that SSM is enabled on the external timing source.

Step 2   Use a test set to determine that the external timing source is delivering SSM.

1.4.117 STU

- Not Alarmed (NA) (Condition)

The synchronization traceability unknown alarm occurs when the reporting node is timed to a reference that does not support synchronization status messaging (SSM), but the ONS 15454 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.

SSM is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET line layer. SSM enables SONET 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 **Sync Messaging** is checked, uncheck the box.

Step 3   If **Sync Messaging** is unchecked, check the box.

Step 4   Click **Apply**.

1.4.118 SWMTXMOD

- Critical, Service affecting

The Switching Matrix Module Failure alarm occurs on the XCVT card or a traffic card. If the alarm reports against a traffic card, it means that the logic component on the cross-connect card is out of frame (OOF) with the logic component on the reporting traffic card. All traffic on the reporting traffic card is lost.

If the alarm reports against an XCVT card, it means that a logic component internal to the reporting XCVT card is out of frame with a second logic component on the same XCVT card. One or more traffic cards may lose traffic as a result of this failure.

Procedure: Clear the SWMTXMOD Alarm

Step 1 If the card reporting the alarm is the standby XCVT card, perform a CTC reset on the standby XCVT:

    a. Display the node view.

    b. Position the cursor over the slot reporting the alarm.

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

    d. Click **Yes** at the **Resetting Card** confirmation dialog.

       Wait for the card to reboot.

    e. If the alarm persists, physically reseat the standby XCVT card.

Step 2 If the card reporting the alarm is the active XCVT card, perform a side switch from the active XCVT card to the standby XCVT card:

    a. Determine the active XCVT 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.

    b. In the node view, choose the **Maintenance > XC Cards** tabs.

    c. Click **Switch**.

    d. Click **Yes** on 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.

    e. Perform a CTC reset on the reporting card:

       From the node view, position the cursor over the slot reporting the alarm.

       Right-click to choose **RESET CARD**.

       Click **Yes** at the **Resetting Card** confirmation dialog.

       Wait for the card to reboot.

    f. If the alarm persists, physically reseat the standby XCVT card.

Step 3   If the card reporting the alarm is an I/O card, perform a side switch from the active cross-connect (XC, XCVT, XC10G) card to the standby cross-connect card:

a.   Determine the active cross-connect (XC, XCVT, XC10G) 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.

b.   In the node view, choose the **Maintenance > XC Cards** tabs.

c.   Click **Switch**.

d.   Click **Yes** on the Confirm Switch dialog box. After the active card goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

e.   If the alarm does not clear after the cross-connect (XC, XCVT, XC10G) side switch, perform a CTC reset on the reporting card:

f.   Display the CTC node view.

g.   Position the cursor over the slot reporting the alarm.

h.   Right-click to choose **RESET CARD.**

i.   Click **Yes** at the **Resetting Card** confirmation dialog.

Wait for the card to reboot.

j.   If the alarm persists, physically reseat the reporting traffic/line card.

1.4.119 SWTOPRI

- Not Alarmed (NA) (Condition)

The synchronization switch to primary reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

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

1.4.120 SWTOSEC

- Not Alarmed (NA) (Condition)

The synchronization switch to secondary reference condition occurs when the ONS 15454 has switched to the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOSEC Condition

Find and troubleshoot alarms related to failures of the primary source, such as the SYNCPRI alarm.

1.4.121 SWTOTHIRD

- Not Alarmed (NA) (Condition)

The synchronization switch to third reference condition occurs when the ONS 15454 has switched to the third timing source (reference 3). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOTHIRD Condition

Find and troubleshoot alarms related to failures of the primary and secondary reference source, such as the SYNCPRI and SYNCSEC alarms.

1.4.122 SYNCPRI

- Minor, Non-service affecting

A loss of timing on primary reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three 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 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 node 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, follow the procedure in the "LOS (BITS)" section on page 1-60.

Step 4   If the primary reference clock is an incoming port on the ONS 15454, follow the procedure in the "LOS (OC-N)" section on page 1-62.

1.4.123 SYNCSEC

- Minor, Non-service affecting

A loss of timing on secondary reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. This switch also triggers the SWTOTHIRD alarm.

Procedure: Clear the SYNCSEC Alarm

Step 1   From the node 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, follow the procedure in the "LOS (BITS)" section on page 1-60.

Step 4 If the secondary timing source is an incoming port on the ONS 15454, follow the procedure in the "LOS (OC-N)" section on page 1-62.

1.4.124 SYNCTHIRD

- Minor, Non-service affecting

A loss of timing on third reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). The ONS 15454 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 uses an internal reference for source three, then the TCC+ card may have failed. The ONS 15454 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SYNCTHIRD Alarm

Step 1 From node view, click the **Provisioning > Timing** tabs.

Step 2 Check the current configuration of the REF-3 for the NE Reference.

Step 3 If the third timing source is a BITS input, follow the procedure in the "LOS (BITS)" section on page 1-60.

Step 4 If the third timing source is an incoming port on the ONS 15454, follow the procedure in the "LOS (OC-N)" section on page 1-62.

Step 5 If the third timing source uses the internal ONS 15454 timing, perform a software reset on the TCC+ card:

    a. Display the CTC node view.

    b. Position the cursor over the slot reporting the alarm.

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

Step 6 If this fails to clear the alarm, physically reseat the TCC+ card.

Step 7 If the reset fails to clear the alarm, replace the TCC+ card.

✎

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

1.4.125 SYSBOOT

- Major, Service affecting

The system reboot alarm indicates that new software is booting on the TCC+ 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.

1.4.126 TIM-P

- Minor, Service affecting

The STS Path Trace Identifier Mismatch Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to manual or Auto for this alarm to occur.

In manual mode at the Path Trace screen, the user types the expected string into the New Expected String field for the receiving port. This string must match the string typed into the New Transmit String field for the sending port. If these fields do not match, the TIM-P alarm will occur. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, this means the circuit path changed or someone typed and entered a new incorrect value into the New Transmit String field. Follow the procedure below to clear either instance.

This alarm also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. This TIM-P occurrence is usually accompanied by other alarms, such as LOS, UNEQ-P, or PLM-P. In this case, reattach or replace the original cables/fibers to clear the alarm.

Procedure: Clear the TIM-P Alarm

Step 1   Log into the circuit source node and select the **Circuits** tab.

Step 2   Select the circuit reporting the alarm, then click **Edit**.

Step 3   At the bottom of the Edit Circuit window, check the **Show Detailed Map** box.

Step 4   On the detailed circuit map, right-click the source circuit port and select **Edit Path Trace** from the shortcut menu.

Step 5   On the detailed circuit map, right click the drop/destination circuit port and select **Edit Path Trace** from the shortcut menu.

Step 6   Compare the New Transmit String and the New Expected String entries in the Path Trace Mode dialog box.

Step 7   If the strings differ, correct the Transmit or Expected strings and click **Apply**.

Step 8   Click **Close**.

1.4.127 TPTFAIL

- Major, Service affecting

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 and not a problem with the port reporting TPTFAIL.

This alarm indicates a problem on either the SONET path or the remote Ethernet port, which prevents the complete end-to-end Ethernet path from working. If there is any SONET path alarm such as AIS-P, LOP-P, UNEQ-P, PDI-P, RDI-P on the SONET path used by the Ethernet port, the affected port raises a TPTFAIL alarm. Also if the far end G1000-4 Ethernet port is administratively disabled or it is seeing a CARLOSS condition it will set the C2 byte in the SONET path overhead to indicate a payload defect condition (PDI-P) which in turn will cause 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. In turn this can also cause the external Ethernet device attached at the near end to detect link down and turn off its transmitter and also cause a CARLOSS condition to occur on this port. In all cases the real problem is either in the SONET path being used by this G1000-4 port or 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 SONET path that this port is using or with the far end G1000-4 port that is mapped to this port. Lookup and troubleshoot any alarms being reported by the OC-N card utilized by the Ethernet circuit of the G1000-4.

Step 2 If no alarms are reported by the OC-N card or a PDI-P condition is reported the problem may 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.

1.4.128 TRMT

- Major, Service affecting

A facility termination equipment transmit failure alarm occurs when there is a transmit failure on the DS1-14 card because of an internal hardware failure. The card must be replaced.

Procedure: Clear the TRMT Alarm

Step 1 Replace the DS1-14 card reporting the failure.

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

Step 2 Call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).

1.4.129 TRMT-MISS

- Major, Service affecting

A facility termination equipment transmitter missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. This means transmit cable is missing on the DS1-14 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector connects to a DS1-14 card instead of a DS-3 card.

Note   DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Procedure: Clear the TRMT-MISS Alarm

Step 1   Check that the device attached to the DS1-14 port is operational.

Step 2   Verify that the cabling is securely connected.

Step 3   Verify that the pinouts are correct.

Step 4   If Steps 1 – 3 do not clear the alarm, replace the transmit cable,.

1.4.130 UNEQ-P

- Critical, Service affecting

An signal label mismatch failure unequipped path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

UNEQ-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment can encompass several consecutive line segments. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15454, often perform the origination and termination tasks of the SONET payload.

A UNEQ-P error message on the ONS 15454 indicates that the node reporting the RFI-P is the terminating node on that path segment.

Note   If you have created a new circuit but it has no signal, an UNEQ-P alarm is reported on the OC-N cards and an AIS-P alarm is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Caution   Deleting a circuit affects traffic.

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

Procedure: Clear the UNEQ-P Alarm

Step 1   Display the CTC network view and right-click the span reporting UNEQ-P.

Step 2   Select **Circuits** from the menu.

Step 3   If the specified circuit is a VT tunnel, check for VTs assigned to the VT tunnel.

Step 4   If the VT tunnel has no assigned VTs, delete the VT tunnel from the list of circuits.

Step 5   If you have complete visibility to all nodes, check for incomplete circuits such as stranded bandwidth from circuits that were not deleted completely.

Step 6   If you find incomplete circuits, verify whether they are working circuits and if they are still passing traffic.

Step 7   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 8   Verify that all circuits terminating in the reporting card are active:

    a.   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. If INCOMPLETE does not change after a full initialization, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 9   After you determine that the port is active, verify the signal source received by the card reporting the alarm.

Step 10   Check the far-end OC-N card that provides STS payload to the card.

Step 11   Verify the far-end cross-connect between the OC-N card and the DS-N card.

Step 12   Clean the far-end optical fiber:

    a.   Clean the fiber according to local site practice.

    b.   If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

1.4.131 UNEQ-V

- Major, Service affecting

An signal label mismatch failure unequipped path alarm indicates that the node is receiving SONET path overhead with bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is the node that is transmitting the VT-level signal into the node reporting the UNEQ-P. The problem node is the next node upstream that processes the signal at the VT level.

The V in UNEQ-V indicates that the failure has occurred at the VT layer. The VT (electrical) layer is created when the SONET signal is broken down into an electrical signal, for example, when an optical signal comes into an ONS 15454, the optical signal is demultiplexed and one of the channels separated from the optical signal is cross connected into an ONS 15454 cross-connect (XC/XCVT/XC10G) card and the corresponding DS-N card.

⚠️

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.**

⚠️

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

Procedure: Clear the UNEQ-V Alarm

Step 1   Verify that all circuits terminating in the reporting card are active:

   a.   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. If INCOMPLETE does not change after full initialization, log on to http://www.cisco.com/tac for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 2   After you determine that the port is active, verify the signal source being received by the DS-N card reporting the alarm.

Step 3   If traffic is being affected, delete and recreate the circuit.

⚠️

Caution   Deleting a circuit can be service affecting.

Step 4   Check the far-end OC-N card that provides STS payload to the DS-N card.

Step 5   Verify the cross-connect between the OC-N card and the DS-N card.

Step 6   Clean the far-end optical fiber:

   a.   Clean the fiber according to local site practice.

   b.   If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 7   Replace OC-N/DS-N cards.

✎

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

1.5 DS3-12E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M23, or C-bit. The choice of framing format affects which line alarms the DS3-12E card reports. The table below lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms as the standard DS-3 card.

Table 1-4   DS3-12E Line Alarms

Alarm	UNFRAMED	M23	CBIT
LOS	◆	◆	◆
AIS	◆	◆	◆
LOF	○	◆	◆
IDLE	○	◆	◆
RAI	○	◆	◆
Terminal Lpbk	◆	◆	◆
Facility Lpbk	◆	◆	◆
FE Lpbk	○	○	◆
FE Common Equipment Failure	○	○	◆
FE Equipment Failure-SA	○	○	◆
FE LOS	○	○	◆
FE LOF	○	○	◆
FE AIS	○	○	◆
FE IDLE	○	○	◆
FE Equipment Failure-NSA	○	○	◆

C H A P T E R **2**

General Troubleshooting

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

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.

- Using the DS3XM-6 Card FEAC (Loopback) Functions—Describes the Far End Alarm and Control (FEAC) features on the DS3XM-6 card.

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

- CTC Operation and Connectivity—Provides troubleshooting procedures for CTC log-in or operation errors and PC and network connectivity.

- Circuits and Timing—Provides troubleshooting procedures for circuit creation, and 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 line (traffic) cards, except Ethernet cards, allow loopbacks and hairpins.

⚠️

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

A facility loopback tests the line interface unit (LIU) of a card, the EIA (electrical interface assembly), 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, the EIA, or cabling plant as the potential cause of a network problem. Figure 2-1 shows a facility loopback on a DS-N card.

Figure 2-1   The facility loopback process on a DS-N card
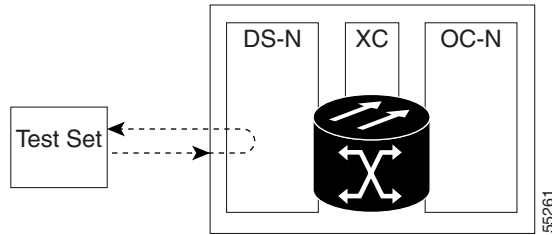
Figure 2-2 shows a facility loopback on an OC-N card.

⚠

Caution   Before performing a facility loopback on an OC-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 containing the loopback OC-N card.

Figure 2-2   The facility loopback process on an OC-N card
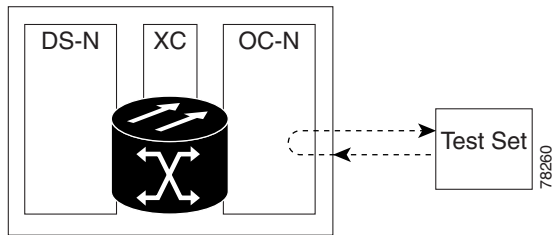
A terminal loopback tests a circuit path as it passes through the cross-connect card (XC, XCVT, or XC10G) and as it loops back from the card being tested. Figure 2-3 shows a terminal loopback on an OC-N card. The test-set traffic comes in on the DS-N card and goes through the cross-connect card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it through the cross-connect card to the DS-N card. This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the OC-N card.

Figure 2-3   The terminal loopback process on an OC-N card
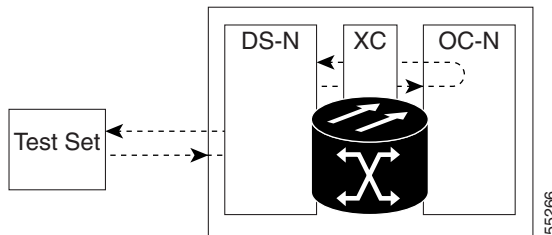
To test the LIU on an OC-N card, connect an optical test set to the OC-N card ports and perform a facility loopback or use a loopback or hairpin on a card that is farther along the circuit path. Figure 2-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the

cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it through the cross-connect card to the OC-N card. This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the DS-N card.

Figure 2-4   The terminal loopback process on a DS-N card
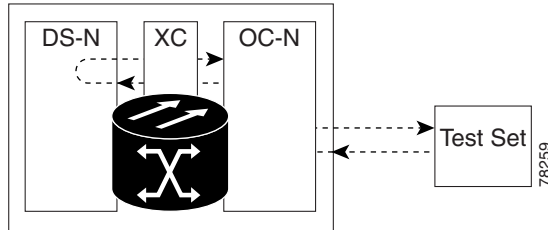
A hairpin circuit brings traffic in and out on a DS-N port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, thus preventing a drop of all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic.

Figure 2-5   The hairpin circuit process on an OC-N card
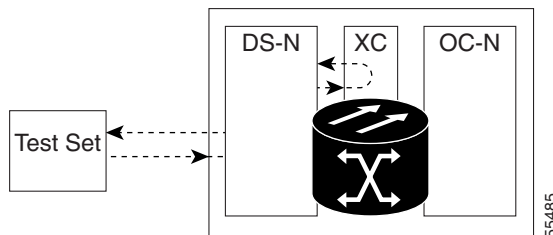
2.2 Identify Points of Failure on a Circuit Path

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 a DS-N circuit on a two-node bidirectional line switched ring (BLSR). 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 DS-N card

2. A hairpin on the source-node DS-N card

3. A terminal loopback on the destination-node DS-N card

4. A facility loopback on the destination DS-N card

✎
Note   All loopback tests require on-site personnel.

2.2.1 Perform a Facility Loopback on a Source DS-N Card

The facility loopback test is performed on the source card in the network circuit, in this example, the DS-N card in the source node. Completing a successful facility loopback on this card eliminates the cabling, the DS-N card, and the EIA as possible failure points. Figure 2-6 shows an example of a facility loopback on a source DS-N card.

Figure 2-6   A facility loopback on a circuit source DS-N card
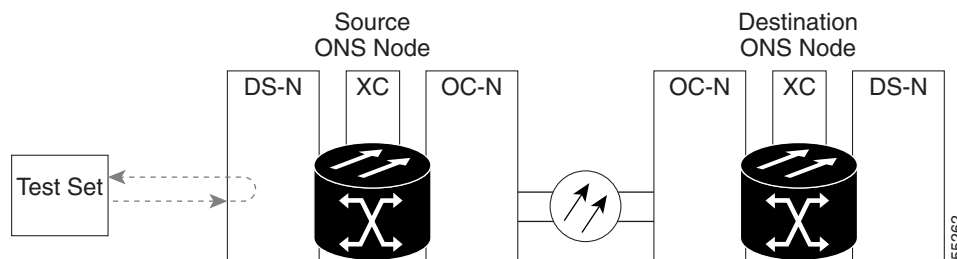
⚠
Caution   Performing a loopback on an in-service circuit is service-affecting.

2.2.1.1 Create the Facility Loopback on the Source DS-N Card

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

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

   d.   Click **Apply**.

   e.   On the confirmation dialog box, click **Yes**.

✎
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.

2.2.1.2 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.

    a. Clear the loopback circuit before testing the next segment of the network circuit path.

    b. Proceed to the "Perform a Hairpin on a Source Node" section on page 2-6.

Step 4   If the test set indicates a faulty circuit, the problem may be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 5   Proceed to the "Test the DS-N Cabling" section on page 2-5.

2.2.1.3 Test the DS-N Cabling

Step 1   Replace the suspect cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

Step 2   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 EIA 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 3   Resend test traffic on the loopback circuit with a known-good cable installed.

Step 4   If the test set indicates a good circuit, the problem was probably the defective cable.

    a. Replace the defective cable.

    b. Clear the loopback circuit before testing the next segment of the network circuit path.

    c. Proceed to the "Perform a Hairpin on a Source Node" section on page 2-6.

Step 5   If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty EIA.

Step 6   Proceed to the "Test the DS-N Card" section on page 2-5.

2.2.1.4 Test the DS-N Card

Step 1   Replace the suspect card with a known-good card. See Card Replacement, page 3-19 for details.

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.

    a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.

    b. Replace the faulty card.

    c. Clear the loopback circuit before testing the next segment of the network circuit path.

    d. Proceed to the "Perform a Hairpin on a Source Node" section on page 2-6.

Step 4   If the test set indicates a faulty circuit, the problem may be a faulty EIA.

**Step 5**   Proceed to the "Test the EIA" section on page 2-6.

2.2.1.5 Test the EIA

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

   a.   Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

   b.   Loosen the nine perimeter screws that hold the EIA panel in place.

   c.   Lift the EIA panel by the bottom to remove it from the shelf assembly.

   d.   Follow the installation procedure for the appropriate EIA. See the EIA Replacement Procedures, page 3-39.

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

Step 3   If the test set indicates a good circuit, the problem was probably an improperly seated EIA.

   a.   Clear the loopback circuit before testing the next segment of the network circuit path.

   b.   Proceed to the "Perform a Hairpin on a Source Node" section on page 2-6

Step 4   If the test set indicates a faulty circuit, the problem is probably the defective EIA.

   a.   Return the defective EIA to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.

   b.   Replace the faulty EIA.

Step 5   Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.

Step 6   If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 7   If the test set indicates a good circuit, the problem was probably the defective EIA.

   a.   Clear the loopback circuit before testing the next segment of the circuit path.

   b.   Proceed to the "Perform a Hairpin on a Source Node" section on page 2-6.

2.2.2 Perform a Hairpin on a Source Node

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card eliminates 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.

Figure 2-7   Hairpin on a source node
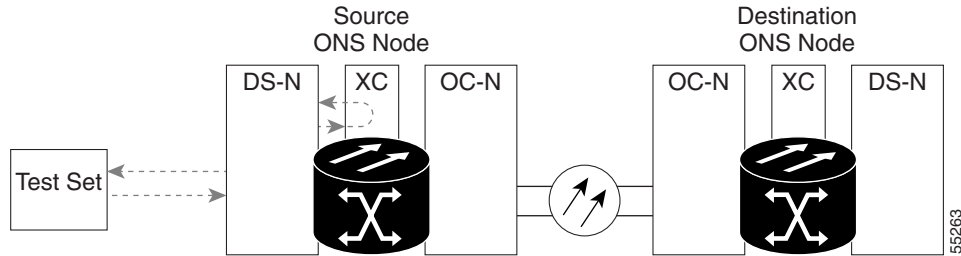
> **Note**   The ONS 15454 does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

2.2.2.1 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 DS-N Card" section on page 2-4, leave the electrical test set hooked up to the DS-N card in the source node.

   b.   If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the EIA 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, fill in the same card and port where the facility loopback test (DS-N card in the source node) was performed and click **Next**.

   f.   In the Circuit Destination dialog box, use the same card and port used for the Circuit Source dialog box and click **Finish**.

Step 3   Confirm that the newly created circuit appears with a direction column indicating that this circuit is one-way.

Step 4   Proceed to the "Test the Hairpin Circuit" section on page 2-8

2.2.2.2 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.

    a.   Clear the hairpin circuit before testing the next segment of the network circuit path.

    b.   Proceed to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 2-9.

Step 4   If the test set indicates a faulty circuit, there may be a problem with the cross-connect card.

Step 5   Proceed to the "Test the Standby Cross-Connect Card" section on page 2-8.

2.2.2.3 Test the Standby Cross-Connect Card

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

    a.   Determine the standby cross-connect card. On both the physical node and the CTC 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 and 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** on 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.

    a.   Clear the loopback circuit before testing the next segment of the network circuit path.

    b.   Proceed to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 2-9.

Step 5   If the test set indicates a good circuit, the problem may be a defective card.

Step 6   To confirm a defective original cross-connect card, proceed to the "Retest the Original Cross-Connect Card" section on page 2-9.

2.2.2.4 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.

    a.   Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case

    b.   Replace the defective cross-connect card. See Switch Traffic and Replace an In-Service Cross-Connect Card, page 3-20for details.

    c.   Clear the loopback circuit before testing the next segment of the network circuit path.

    d.   Proceed to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 2-9

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.

    a.   Clear the loopback circuit before testing the next segment of the network circuit path.

    b.   Proceed to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 2-9.

2.2.3 Perform a Terminal Loopback on a Destination DS-N Card

This test is a terminal loopback performed on the destination line card in the circuit, in the following example the DS-N card in the destination node. First, create a bidirectional circuit that starts on the source node DS-N port and terminates on the destination node DS-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a destination node DS-N card verifies that the circuit is good up to the destination DS-N. Figure 2-8 shows an example of a terminal loopback on a destination DS-N card.

Figure 2-8   Terminal loopback on a destination DS-N card
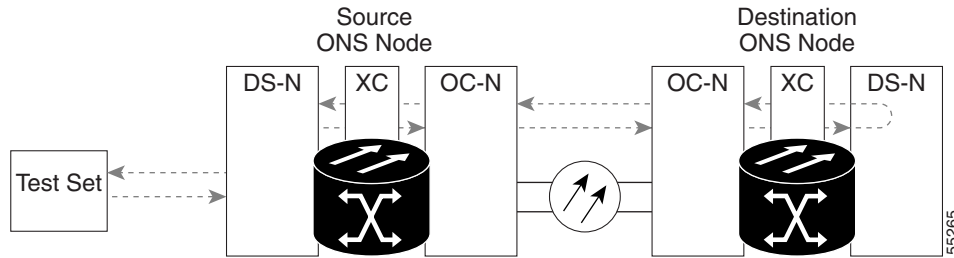
⚠ **Caution**   Performing a loopback on an in-service circuit is service-affecting.

2.2.3.1 Create the Terminal Loopback on a Destination DS-N Card

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

  a.   If you just completed the "Perform a Hairpin on a Source Node" section on page 2-6, leave the electrical test set hooked up to the DS-N card in the source node.

  b.   If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both transmit (Tx) and receive (Rx) 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 "DSNtoDSN".

  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 card and port where the facility loopback test (the DS-N card in the source node) was performed and click **Next**.

  f.   In the Circuit Destination dialog box, fill in the destination card and port (the DS-N card in the destination node) and click **Finish**.

Step 3   Confirm that the newly created circuit appears on a Circuits screen row with a direction column that shows a two-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 loopback circuit on the destination card and port being tested:

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

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

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

    d. Click **Apply**.

    e. On the confirmation dialog box, click **Yes**.

Step 5   Proceed to the "Test the Terminal Loopback Circuit on the Destination DS-N Card" section on page 2-11.

2.2.3.2 Test the Terminal Loopback Circuit on the Destination DS-N 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.

    Proceed to the "Perform a Facility Loopback on a Destination DS-N Card" section on page 2-11.

Step 4   If the test set indicates a faulty circuit, the problem may be a faulty card.

    Proceed to the "Test the Destination DS-N Card" section on page 2-11.

2.2.3.3 Test the Destination DS-N Card

Step 1   Replace the suspect card with a known-good card. See Card Replacement, page 3-19 for details.

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

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

    a. Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.

    b. Replace the defective DS-N card.

Step 4   Proceed to the "Perform a Facility Loopback on a Destination DS-N Card" section on page 2-11.

2.2.4 Perform a Facility Loopback on a Destination DS-N Card

The final test is a facility loopback performed on the last card in the circuit, in this case the DS-N card in the destination node. Completing a successful facility loopback on this card eliminates the possibility that the destination node cabling, DS-N card, LIU, or EIA is responsible for a faulty circuit. Figure 2-9 shows an example of a facility loopback on a destination DS-N card.

Figure 2-9   Facility loopback on a destination DS-N card

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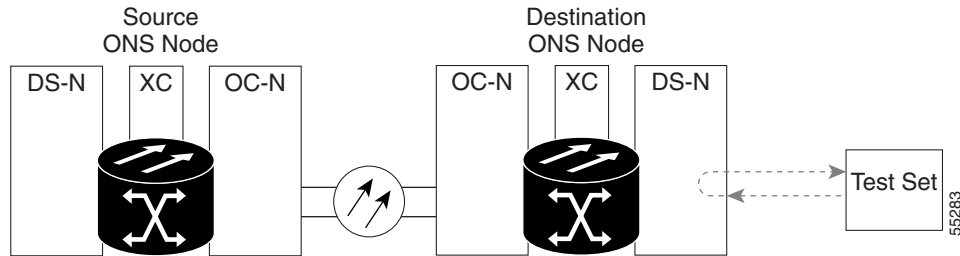
Caution   Performing a loopback on an in-service circuit is service-affecting.

2.2.4.1 Create a Facility Loopback Circuit on a Destination DS-N Card

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

Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the EIA connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Set up your 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.   On the confirmation dialog box, click **Yes**.

✎

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 2-12.

2.2.4.2 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.

   a.   Clear the facility loopback.

b. The entire DS-N 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 DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 5 Proceed to the "Test the DS-N Cabling" section on page 2-5.

2.2.4.3 Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

Step 2 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 EIA 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 3 Resend test set traffic on the loopback circuit with a known-good cable installed.

Step 4 If the test set indicates a good circuit, the problem was probably the defective cable.

a. Replace the defective cable.

b. Clear the loopback circuit.

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

Step 5 If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty EIA.

Step 6 Proceed to the "Test the DS-N Card" section on page 2-5.

2.2.4.4 Test the DS-N Card

Step 1 Replace the suspect card with a known-good card.

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.

a. Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.

b. Replace the faulty card. See Card Replacement, page 3-19 for details.

c. Clear the loopback circuit.

d. The entire DS-N 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 EIA.

Step 5 Proceed to the "Test the EIA" section on page 2-6.

2.2.4.5 Test the EIA

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

    a.   Remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454, and pull it away from the shelf assembly.

    b.   Loosen the nine perimeter screws that hold the EIA panel in place.

    c.   Lift the EIA panel by the bottom to remove it from the shelf assembly.

    d.   Follow the installation procedure for the appropriate EIA. See the "Electrical Interface Assembly Replacement" section on page 3-38.

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

Step 3   If the test set indicates a good circuit, the problem was probably an improperly seated EIA.

    a.   Clear the loopback circuit.

    b.   The entire DS-N 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 EIA.

    a.   Return the defective EIA to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.

    b.   Replace the faulty EIA.

Step 5   Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.

Step 6   If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

    If the faulty circuit persists, call Cisco TAC at 1-877-323-7368 for assistance.

Step 7   If the test set indicates a good circuit, the problem was probably the defective EIA.

    a.   Clear the loopback circuit.

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

2.2.5 Using the DS3XM-6 Card FEAC (Loopback) Functions

The DS3XM-6 card supports Far End Alarm and Control (FEAC) features that are not available on basic DS-3 cards. Click the Maintenance tab at the DS3XM-6 card view to reveal the two additional DS3XM-6 columns. Figure 2-10 shows the DS3 subtab and the additional *Send Code* and *Inhibit FE Lbk* columns.

Figure 2-10   Accessing FEAC functions on the DS3XM-6 card
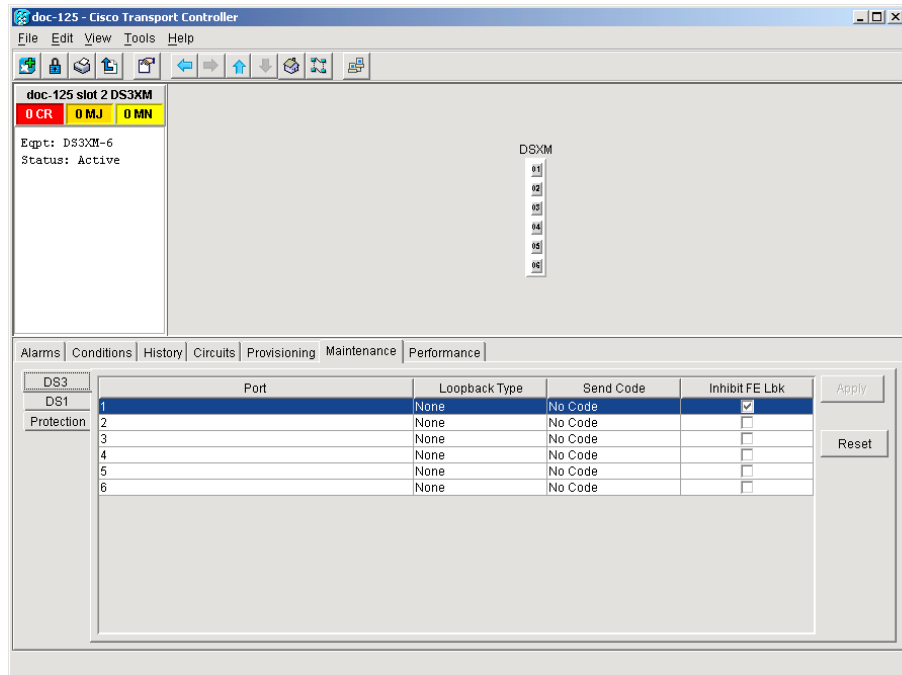
The far end in FEAC refers to the piece of equipment that is connected to the DS3XM-6 card and not the far end of a circuit. In Figure 2-11, if a DS3XM-6 (near-end) port is configured to send a Line Loop Code, the code will be sent to the connected test set, not the DS3XM-6 (far-end) port.

Figure 2-11   Diagram of far end action code
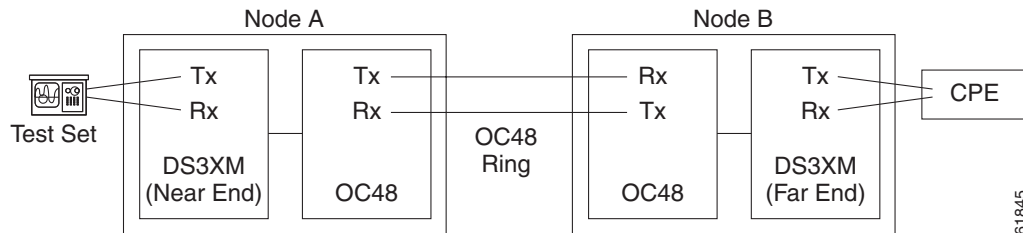
2.2.5.1 FEAC Send Code

The Send Code column on the maintenance tab of a DS3XM-6 port only applies to in-service ports configured for CBIT framing. The column lets a user select No Code (the default) or Line Loop Code. Selecting Line Loop Code inserts a line loop activate FEAC (Far End Alarm and Control) in the CBIT overhead transmitting to the connected facility. This code initiates a loopback from the facility to the ONS 15454. Selecting No Code sends a line-loop-deactivate FEAC code to the connected equipment, which will remove the loopback. You can also insert a FEAC for the 28 individual DS-1 circuits transmuxed into a DS-3 circuit.

2.2.5.2 FEAC Inhibit Loopback

The DS3XM-6 ports and transmuxed DS-1s initiate loopbacks when they receive FEAC Line Loop codes. If the Inhibit Loopback checkbox is checked for a DS-3 port, then that port will ignore any received FEAC Line Loop codes and will not loop back. The port can still be put into loopback manually using the Loopback Type column even if the Inhibit Loopback box is selected. Only DS-3 ports can be configured to inhibit responses to FEAC loopback commands, individual DS-1 ports cannot inhibit their responses.

2.2.5.3 FEAC Alarms

The node raises a LPBKDS3FEAC-CMD or LPBKDS1FEAC-CMD alarm for a DS-1 or DS-3 port if a FEAC loopback code is sent to the far end.

If the ONS 15454 port is in loopback from having received a loopback activate FEAC code, a LPBKDS3FEAC or LPBKDS1FEAC alarm occurs. The alarm will clear when a loopback deactivate FEAC command is received on that port.

A DS3E card will respond to, and can inhibit, received FEAC DS3 level loopback codes. A DS3E card cannot be configured to send FEAC codes.

2.3 CTC Operation and Connectivity

This section contains troubleshooting procedures for CTC login or operation errors and PC and network connectivity.

2.3.1 Operation: Unable to Change Node View to Network View

Symptom: When activating a large, multi node BLSR with a software upgrade, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

Table 2-1 describes the potential cause(s) of the symptom and the solution(s).

Table 2-1   Browser Stalls When Downloading Files From TCC+

Possible Problem	Solution
The large, multi node BLSR requires more memory for the GUI environment variables.	Reset the system or user CTC_HEAP environment variable to increase the memory limits.
	See the "Reset the CTC_HEAP Environment Variable for Windows" section on page 2-17 or the "Reset the CTC_HEAP Environment Variable for Solaris" section on page 2-17 to enable the CTC_HEAP variable change.
	Note This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

2.3.1.1 Reset the CTC_HEAP Environment Variable for Windows

Step 1   Exit any and all open and running CTC and Netscape applications.

Step 2   From the Windows Desktop, right-click on My Computer and choose **Properties** in the pop-up menu.

Step 3   In the System Properties window, click the **Advanced** tab.

Step 4   Click the **Environment Variables** button to open the Environment Variables window.

Step 5   Click the **New** button under the User variables field or the System variables field.

Step 6   Type CTC_HEAP in the Variable Name field.

Step 7   Type *256* in the Variable Value field, and then click **OK** to create the variable.

Step 8   Click **OK** in the Environment Variables window to accept the changes.

Step 9   Click **OK** in the System Properties window to accept the changes.

You may now restart the browser and CTC software.

2.3.1.2 Reset the CTC_HEAP Environment Variable for Solaris

Step 1   From the user shell window, kill any CTC applications.

Step 2   Kill any Netscape applications.

Step 3   In the user shell window, set the environment variable to increase the heap size: % setenv CTC_HEAP 256

You may now restart the browser and CTC software in the same user shell window.

2.3.2 Operation: Browser Stalls When Downloading CTC JAR Files From TCC+

Symptom: The browser stalls or hangs when downloading a CTC JAR file from the TCC+ card.

Table 2-2 describes the potential cause(s) of the symptom and the solution(s).

Table 2-2   Browser Stalls When Downloading jar File From TCC+

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 2-18.

2.3.2.1 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.

2.3.3 Operation: CTC Does Not Launch

Symptom: CTC does not launch, usually an error message appears before the login screen displays.

Table 2-3 describes the potential cause(s) of the symptom and the solution(s).

Table 2-3   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 2-18.

2.3.3.1 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.

2.3.4 Operation: Sluggish CTC Operation or Login Problems

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

Table 2-4 describes the potential cause(s) of the symptom and the solution(s).

Table 2-4   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 to download a new set of jar files to your computer hard drive. See the "Delete the CTC Cache File Automatically" section on page 2-19 or the "Delete the CTC Cache File Manually" section on page 2-20.

2.3.4.1 Delete the CTC Cache File Automatically

Step 1   Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2   Close all open CTC sessions and browser windows. The PC operating system 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 2-12 shows the Delete CTC Cache screen.

Note   For CTC releases prior to 3.0, automatic deletion is unavailable. For CTC Cache file manual deletion, see the Delete the CTC Cache File Manually

Figure 2-12   Deleting the CTC cache
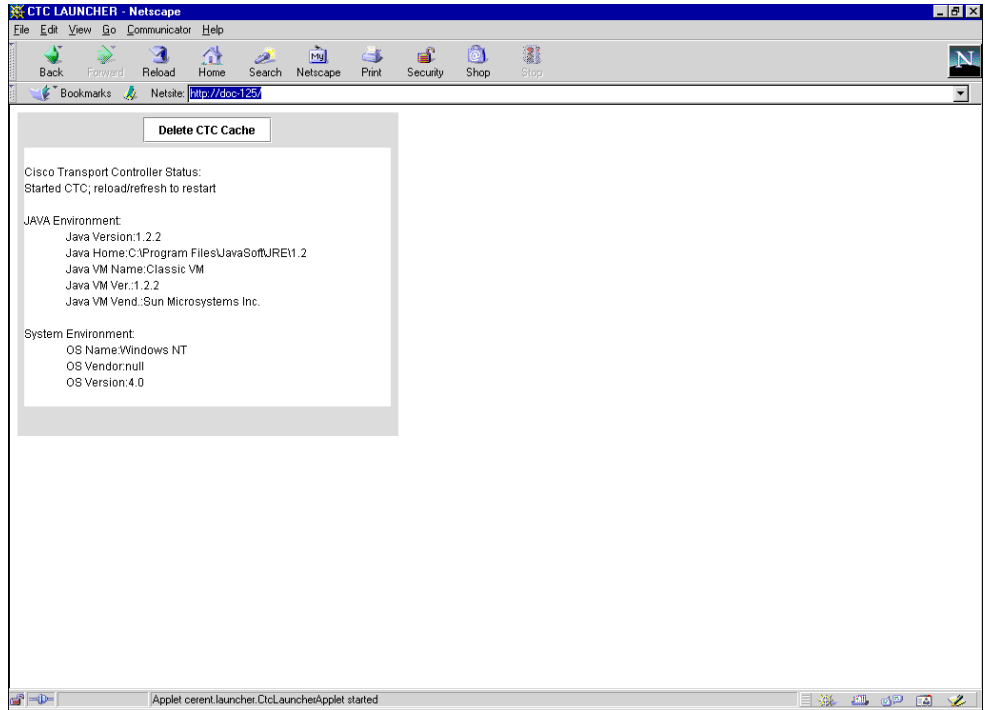
2.3.4.2 Delete the CTC Cache File Manually

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+. 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.

2.3.5 Operation: 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 2-5 describes the potential cause(s) of the symptom and the solution(s).

Table 2-5   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 "Operation: Different CTC Releases Do Not Recognize Each Other" section on page 2-23.
A username/password mismatch.	Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the "Operation: Username or Password Do Not Match" section on page 2-24.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "Ethernet Connections" section on page 2-27.
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" section on page 1-33.

2.3.6 Operation: 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 2-6 describes the potential cause(s) of the symptom and the solution(s).

Table 2-6   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 software CD. This file is installed when you run the CTC Setup Wizard (refer to the CTC installation information in the *Cisco ONS 15454 Installation and Operations Guide* for instructions). 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 2-21.

2.3.6.1 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.

2.3.7 Operation: Java Runtime Environment Incompatible

Symptom: The CTC application will not run properly.

Table 2-7 describes the potential cause(s) of the symptom and the solution(s).

Table 2-7   Java Runtime Environment Incompatible

Possible Problem	Solution
Do not have the compatible 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 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. See the "Launch CTC to Correct the Core Version Build" section on page 2-23.
	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 2-8 shows JRE compatibility with ONS 15454 software releases.

Table 2-8   JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15454 Release 2.2.1 and earlier	Yes	No
ONS 15454 Release 2.2.2	Yes	Yes
ONS 15454 Release 3.0	Yes	Yes
ONS 15454 Release 3.1	Yes	Yes
ONS 15454 Release 3.2	Yes	Yes

2.3.7.1 Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser will download the jar file from CTC.

> **Note** After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15454 and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 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.

2.3.8 Operation: Different CTC Releases Do Not Recognize Each Other

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

Table 2-9 describes the potential cause(s) of the symptom and the solution(s).

Table 2-9   Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the TCC+ card are incompatible.	This occurs when the TCC+ 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.
	Note Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node will not recognize the new node.
	See the "Launch CTC to Correct the Core Version Build" section on page 2-23.

2.3.8.1 Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser will download the jar file from CTC.

> ✎
>
> **Note**   After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15454 and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 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.

2.3.9 Operation: Username or Password Do Not Match

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

Table 2-10 describes the potential cause(s) of the symptom and the solution(s).

Table 2-10   Username or Password Do Not Match

Possible Problem	Solution
The username or password entered do not match the information stored in the TCC+.	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, type the *CISCO15* user name in capital letters and click **Login** (no password is required). If you are using a CTC software release prior to 3.0 and CISCO15 does not work, type *cerent454* for the user name.
	See the "Verify Correct Username and Password" section on page 2-24.

2.3.9.1 Verify Correct Username and Password

Step 1   Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.

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

Step 3   Call Cisco TAC at 1-877-323-7368 to have them enter your system and create a new user name and password.

2.3.10 Operation: No IP Connectivity Exists Between Nodes

Symptom: The nodes have a grey icon and is usually accompanied by alarms.

Table 2-11 describes the potential cause(s) of the symptom and the solution(s).

Table 2-11   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 2-27.

2.3.11 Operation: 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 2-12 describes the potential cause(s) of the symptom and the solution(s).

Table 2-12   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 "EOC" section on page 1-33.

2.3.12 Operation: 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 2-13 describes the potential cause(s) of the symptom and the solution(s).

Table 2-13   Browser Login Does Not Launch Java

Possible Problem	Solution
The PC operating system and browser are not properly configured.	Reconfigure the PC operating system and the browser. See the "Reconfigure the PC Operating System and the Browser" section on page 2-25.

2.3.12.1 Reconfigure the PC Operating System and the Browser

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 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   Double-click the **Java Plug-in 1.3.1_02** icon.

Step 5   Click **Advanced** 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 **Apply**.

Step 8   On Netscape Navigator, click **Edit > Preferences**.

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

Step 10   Again on Netscape Navigator, click **Edit > Preferences**.

Step 11   Click **Advanced > Cache**.

Step 12   Confirm that the Disk Cache Folder field shows C:\ProgramFiles\Netscape\Communicator\cache for
Windows 95/98/ME

or C:\ProgramFiles\Netscape\<username>\Communicator\cache for Windows NT/2000.

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

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

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

Step 16   Temporarily disable any virus-scanning software on the computer. See the "Operation: Browser Stalls
When Downloading CTC JAR Files From TCC+" section on page 2-17.

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

Step 18   Restart the browser and log into the ONS 15454.

2.3.13 Connectivity: Verify PC Connection to ONS 15454 (ping)

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

Table 2-14 describes the potential cause(s) of the symptom and the solution(s).

Table 2-14   Verify PC connection to ONS 15454 (ping)

Possible Problem	Solution
A lost connection between the PC and the ONS 1554.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC+ card. A ping command will work if the PC connects directly to the TCC+ card or uses a LAN to access the TCC+ card.
	Note Software Release 3.0 requires the TCC+ card and does not support the TCC card. Releases 2.2, 2.2.1, and 2.2.2 support the TCC and the TCC+ cards.
	See the "Ping the ONS 15454" section on page 2-27.

2.3.13.1 Ping the ONS 15454

Step 1   Display the command prompt:

a.   If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, 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 IP address]
For example, ping 192.1.0.2.
```

Step 3   If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message 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 through a LAN, check that the workstation's IP address is on the same subnet as the ONS node.

Step 6   If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation's NIC is illuminated.

2.3.14 Calculate and Design IP Subnets

Symptom: You cannot calculate or design IP subnets on the ONS 15454.

Table 2-15 describes the potential cause(s) of the symptom and the solution(s).

Table 2-15   Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15454 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 IP capability, refer to the *Cisco ONS 15454 Reference Manual.*

2.3.15 Ethernet Connections

Symptom: Ethernet connections appear to be broken or are not working properly.

Table 2-15 describes the potential cause(s) of the symptom and the solution(s).

Table 2-16   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 2-13 when consulting the steps in the "Verify Ethernet Connections" section on page 2-28.
Incorrect connections.	

Figure 2-13   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
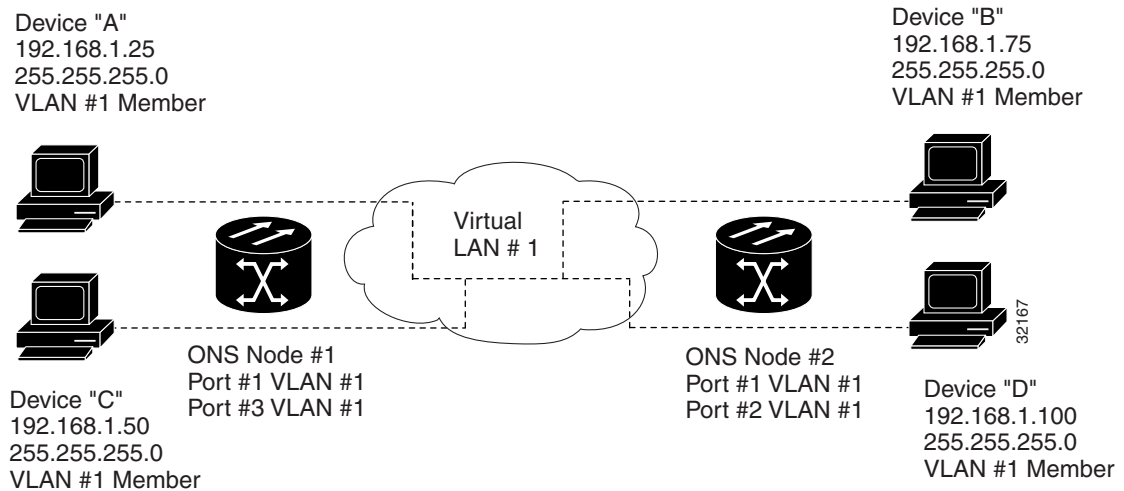
2.3.15.1 Verify Ethernet Connections

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 #1 and Ports 1 and 2 on ONS 15454 #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 15454s and the attached device.

   b. Verify that the ports are enabled on the Ethernet cards.

   c. Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

   d. Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.

   e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Run the procedure in the "Lamp Test for Card LEDs" section on page 2-46.

Step 6 Verify connectivity between device A and device C by pinging between these locally attached devices (see the "Connectivity: Verify PC Connection to ONS 15454 (ping)" section on page 2-26). 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 #1 and ONS 15454 #2 ports also use VLAN #1.

2.3.16 VLAN Cannot Connect to Network Device from Untag Port

Symptom: Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag may have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 2-14). They may also see a higher than normal runt packets count at the network device attached to the Untag port.

Figure 2-14   A VLAN with Ethernet ports at Tagged and Untag
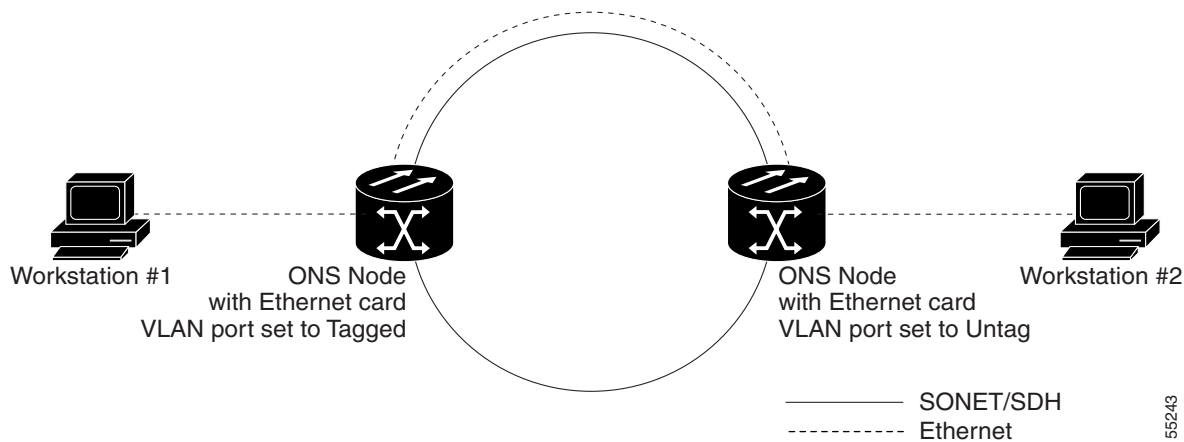
Table 2-14 describes the potential cause(s) of the symptom and the solution(s).

Table 2-17   Verify PC connection to ONS 15454 (ping)

Possible Problem	Solution
The Tagged ONS 15454 adds the 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.	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.	

2.3.16.1 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 2-15).

Figure 2-15   Configuring VLAN membership for individual Ethernet ports
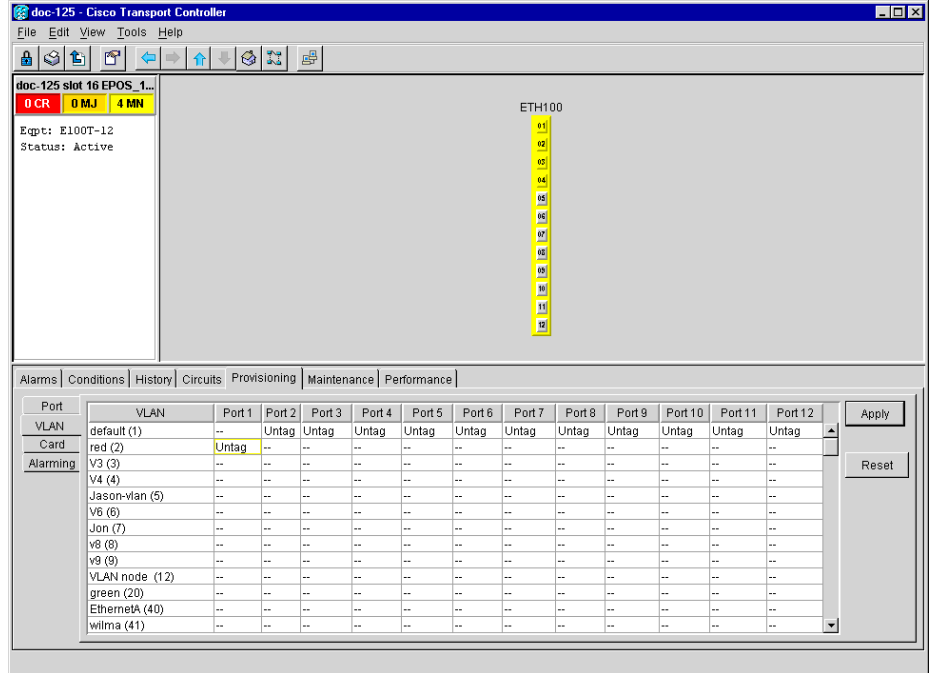
Step 3   If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.

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**.

2.3.17 Operation: Cross-Connect Card Oscillator Fails

Symptom: The XC, XCVT, or XC10G card can be affected by this problem. It is indicated by a CTNEQPT-PBSTBY or CTNEQPT-PBACT 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

- SD-L against near-end or far-end line cards

- AIS-L against far-end line cards

- RFI-L against near-end line cards

Table 2-18 describes the potential cause(s) of the symptom and the solution(s).

Table 2-18   Cross-Connect Card Oscillator Fails

Possible Problem	Solution
The XC, XCVT, or 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 2-32. 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 2-32.

2.3.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active

Step 1 If the CTNEQPT-PBSTBY 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-PBSTBY does not clear, replace the Slot 10 cross-connect card with a spare card.

Step 5 If CTNEQPT-PBSTBY 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-PBACT condition raised against all I/O cards in the node, verify that CTNEQPT-PBSTBY has cleared on all I/O cards. Seeing CTNEQPT-PBACT 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-PBACT condition has cleared on all I/O cards.

Step 9 If you see CTNEQPT-PBSTBY 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-PBSTBY condition has cleared on all I/O cards.

2.3.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active

Step 1 If the CTNEQPT-PBACT 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-PBACT 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-PBACT 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-PBACT condition has cleared on all I/O cards.

Step 9   If you then see the CTNEQPT-PBSTBY condition raised against all I/O cards, verify that CTNEQPT-PBACT 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-PBSTBY condition has cleared on all I/O cards.

2.4 Circuits and Timing

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

2.4.1 AIS-V on DS3XM-6 Unused VT Circuits

Symptom: An incomplete circuit path causes an alarm indications signal (AIS).

Table 2-19 describes the potential cause(s) of the symptom and the solution(s).

Table 2-19   Calculate and Design IP Subnets

Possible Problem	Solution
The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.	An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth. Perform the "Clear AIS-V on DS3XM-6 Unused VT Circuits" section on page 2-33.

2.4.1.1 Clear AIS-V on DS3XM-6 Unused VT Circuits

Step 1   Determine the affected port.

Step 2   Record the node ID, slot number, port number, or VT number.

Step 3   Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

Step 4   Uncheck the bidirectional box in the circuit creation window.

Step 5   Give the unidirectional VT circuit an easily recognizable name, such as `delete me`.

Step 6   Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** tabs.

Step 7   Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

Step 8   From the Loopback Type list, choose **Facility (line)** and click **Apply**.

Step 9   Click **Circuits**.

Step 10 Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**.

Step 11 Click **Yes** in the Delete Confirmation box.

Step 12 Display the DS3XM-6 card in CTC card view. Click **Maintenance > DS1**.

Step 13 Locate the VT in Facility (line) Loopback.

Step 14 From the Loopback Type list, choose **None** and then click **Apply**.

Step 15 Click the **Alarm** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the DS3XM-6 cards.

2.4.2 Circuit Creation Error with VT1.5 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 VT1.5 circuit in CTC.

Table 2-20 describes the potential cause(s) of the symptom and the solution(s).

Table 2-20   Circuit Creation Error with VT1.5 Circuit

Possible Problem	Solution
You may have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message.	The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations will exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a UPSR or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Guide* for more information.

2.4.3 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card

Symptom: You cannot create a circuit from a DS-3 card to a DS3XM-6 card.

Table 2-21 describes the potential cause(s) of the symptom and the solution(s).

Table 2-21   Unable to Create Circuit from DS-3 Card to DS3XM-6 Card

Possible Problem	Solution
A DS-3 card and a DS3XM-6 card have different functions.	A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. Thus you can create a circuit from a DS3XM-6 card to a DS-1 card, but not from a DS3XM-6 card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 has a VT payload with a C2 hex value of 02. **Note** You can find instructions for creating circuits in the *Cisco ONS 15454 Installation and Operations Guide*.

2.4.4 DS3 Card Does Not Report AIS-P From External Equipment

Symptom: A DS3-12/DS3N-12/DS3-12E/DS3N-12E card does not report STS AIS-P from the external equipment/line side.

Table 2-22 describes the potential cause(s) of the symptom and the solution(s).

Table 2-22   DS3 Card Does Not Report AIS-P From External Equipment

Possible Problem	Solution
The card is functioning as designed.	This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side.
	DS3-12/DS3N-12E cards have DS3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information on the PM capabilities of the DS3-12E/DS3N-12E cards, refer to the *Cisco ONS 15454 Installation and Operations Guide*.

2.4.5 OC-3 and DCC Limitations

Symptom: Limitations to OC-3 and DCC usage.

Table 2-23 describes the potential cause(s) of the symptom and the solution(s).

Table 2-23   OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the ONS 15454.	For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Installation and Operations Guide*.

2.4.6 ONS 15454 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 Switches Timing Reference

Possible Problem	Solution
The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.	The ONS 15454 internal clock operates at a Stratum 3 level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of ± 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or $3.7x10^{-7}$/day, including temperature.

ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source. |
The optical or BITS input is not functioning.	
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.	

2.4.7 Holdover Synchronization Alarm

Symptom: The clock is running at a different frequency than normal and the HLDOVERSYNC 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 "HLDOVERSYNC" section on page 1-49 for a detailed description of this alarm.

Note   The ONS 15454 supports holdover timing per Telcordia standard GR-4436 when provisioned for external (BITS) timing. |

2.4.8 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 1-48 for a detailed description of this alarm.

2.4.9 Daisy-Chained BITS Not Functioning

Symptom: You are unable to daisy-chain the BITS.

Table 2-27 describes the potential cause(s) of the symptom and the solution(s).

Table 2-27   Daisy-Chained BITS Not Functioning

Possible Problem	Solution
Daisy-chaining BITS is not supported on the ONS 15454.	Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

2.5 Fiber and Cabling

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

2.5.1 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. 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 2-38.

2.5.2 Faulty Fiber-Optic Connections

Symptom: A line card has multiple SONET 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 SONET alarms and signal errors. See the "Verify Fiber-Optic Connections" section on page 2-38.
Faulty gigabit interface connectors.	Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the "Replace Faulty Gigabit Interface Converters" section on page 2-40.
Faulty CAT-5 cables.	Faulty CAT-5 cables can be the source of SONET alarms and signal errors. See the "Crimp Replacement CAT-5 Cables" section on page 2-42.

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.**

2.5.2.1 Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.

SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3   Check that the single-mode fiber power level is within the specified range:

    a.   Remove the 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 2-43.

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 OC-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 OC-N card you are working on and the far-end card.

    c.   Ensure that the far-end transmitting card is not an ONS intermediate range (IR) card when an ONS long range (LR) card is appropriate.

       IR cards transmit a lower output power than LR cards.

    d.   Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

    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 OC-N card you are working on and the far-end card.

    c.   Retest the fiber power level.

    d.   If the replacement fiber still shows no power, replace the 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 OC-N card.

Receiver overloads occur when maximum receiver power is exceeded.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the ONS OC-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS OC-N cards. Refer to the attenuator documentation for specific instructions.

Tip Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

2.5.2.2 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, 15454-GBIC-SX, one for long-reach applications, 15454-GBIC-LX, and one for ultra-long-reach applications, 15454-GBIC-ZX.

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 a Gigabit Ethernet (E1000-2/E1000-2-G or G1000-4) card. Figure 2-16 shows a GBIC.

Figure 2-16   A gigabit interface converter (GBIC)

Receiver   Transmitter
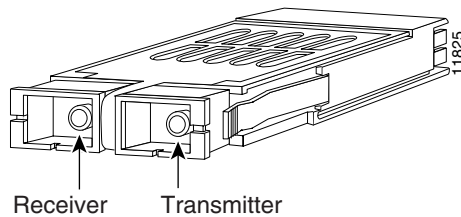
Warning **Class 1 laser product**

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 card.

✎

Note   GBICs are keyed to prevent incorrect installation.

Figure 2-17   Installing a GBIC on the E1000-2/E1000-2-G card
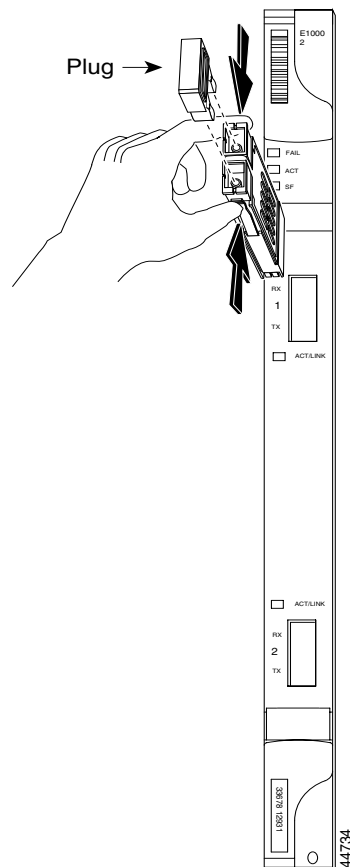
Step 7   Slide the GBIC through the front flap until you hear a click.

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.

2.5.2.3 Crimp Replacement CAT-5 Cables

You can crimp your own CAT-5 cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a straight-through cable when connecting an ONS 15454 to a router or workstation. Use CAT 5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 2-18 shows the layout of an RJ-45 connector. Figure 2-19 shows the layout of a straight-through cable and Figure 2-20 shows the layout of a cross-over cable.

Figure 2-18   RJ-45 pin numbers
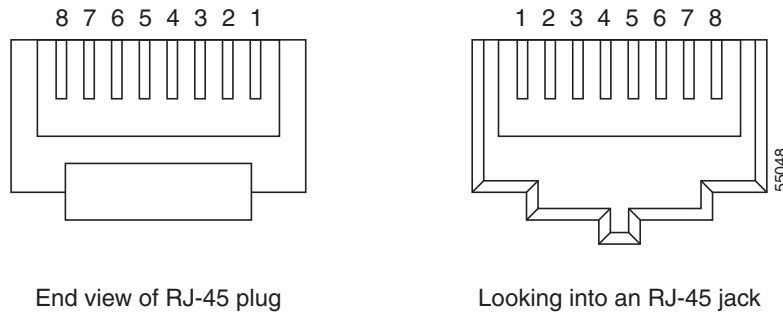
End view of RJ-45 plug   Looking into an RJ-45 jack

Figure 2-19   A straight-through cable layout
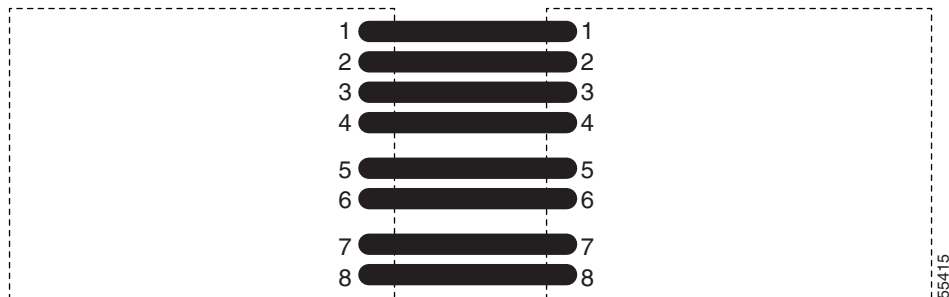
Table 2-30   Straight-through cable pinout

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

Figure 2-20   A cross-over cable layout
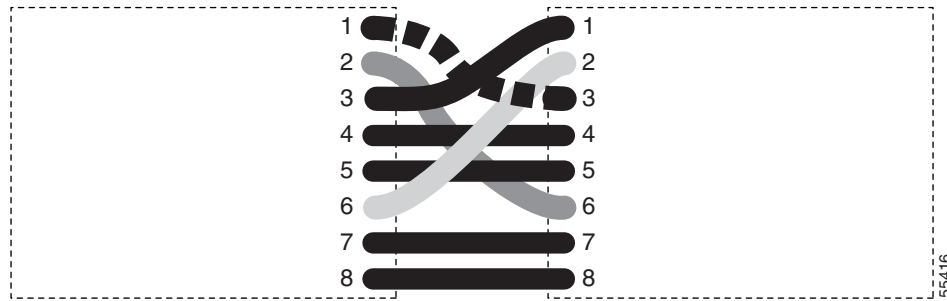
Table 2-31   Cross-over cable pinout

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.

2.5.3 Optical Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate.

Table 2-32   Optical Card Transmit and Receive Levels

Optical card	Rx	Tx
OC3 IR 4/STM1SH 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 IR/STM4 SH 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 LR/STM4 LH 1310	–8 to –28 dBm	+2 to –3 dBm
OC12 LR/STM4 LH 1550	–8 to –28 dBm	+2 to –3 dBm
OC48 IR 1310	0 to –18 dBm	0 to –5 dBm
OC48 LR 1550	–8 to –28 dBm	+3 to –2 dBm
OC48 AS LR 1550	–8 to –28 dBm	+3 to –2 dBm
OC48 ELR DWDM	–8 to –28 dBm	0 to –2 dBm
OC192 LR 1550	–9 to –17 dBm	+10 to +7 dBm

2.6 Power and LED Tests

This section provides the "Power Supply Problems" section on page 2-44, the "Power Consumption for Node and Cards" section on page 2-45, and the "Lamp Test for Card LEDs" section on page 2-46.

2.6.1 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. Improperly connected power supply.	The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC.
	A newly installed ONS 15454 that is not properly connected to its power supply will not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site.
	A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General** tabs and change the *Date* and *Time* fields.
	See the "Isolate the Cause of Power Supply Problems" section on page 2-44.

⚠ **Caution**   Operations that interrupt power supply or short the power connections to the ONS 15454 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. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.**

2.6.1.1 Isolate the Cause of Power Supply Problems

Step 1   If a single ONS 15454 show signs of fluctuating power or power loss:

  a. Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.

  b. Verify that the power cable is #12 or #14 AWG and in good condition.

    c. Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.

    d. Verify that 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 EIA. Connect this cable to the ground terminal according to local site practice.

    g. Verify that the DC power source has enough capacity to carry the power load.

    h. If the DC power source is battery-based:

       – Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.

       – Check the age of the batteries. Battery performance decreases with age.

       – Check for opens and shorts in batteries, which 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.

2.6.2 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 Installation and Operations Guide*.

2.6.3 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 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order.
	See the "Verify Card LED Operation" section on page 2-46.

2.6.3.1 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 light up, the LED is faulty. Call the Cisco TAC at 1-877-323-7368 and fill out an RMA to return the card.

C H A P T E R 3

Maintenance

This chapter describes maintenance information and procedures for Cisco ONS 15454, including:

- Air filter inspection and replacement
- Fan-tray assembly replacement
- Alarm interface panel replacement
- System reset
- Database backup and restore
- Reverting to an earlier software load
- Card replacement
- TCC card to TCC+ card upgrade
- XC card to XCVT card upgrade
- XC/XCVT card to XC10G card upgrade
- DS3/DS3N card to DS3E/DS3EN card upgrade
- Span upgrades
- Protection group switching
- Electrical interface assembly (EIA) replacement
- Fiber cleaning
- Powering down a node

3.1 Air Filter Inspection and Replacement

The ONS 15454 contains an air filter that you should remove and visually inspect approximately every 30 days, depending on the cleanliness of the operating environment. NEBS 3E and later versions of the ONS 15454 use a reusable air filter that is installed either beneath the fan-tray assembly or in the optional external filter brackets. Earlier versions of the ONS 15454 use a disposable air filter that is installed beneath the fan-tray assembly only. For more information about filter brackets and air filter installation, see the "Installation" chapter of the *Cisco ONS 15454 Installation and Operations Guide.*

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

3.1.1 Reusable Air Filter

The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter. Figure 3-1 illustrates a reusable fan-tray air filter in an external filter bracket. When the filter is dirty, remove the filter and clean it by either vacuuming the filter or running water through it. Because the filter material is delicate, only a very low-power vacuum should be used. If you are cleaning with water, make sure the filter is completely dry (dry time is at least eight hours) before replacing it in the fan-tray assembly. Spare filters should be kept in stock.

Figure 3-1   A reusable fan-tray air filter in an external filter bracket

Fan tray filter
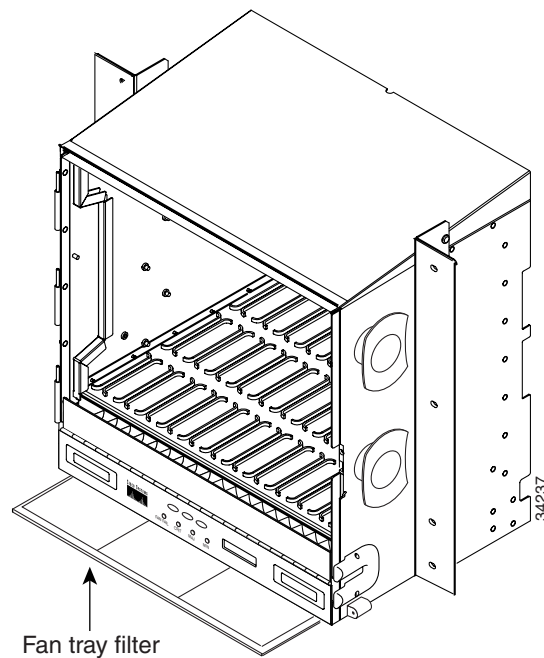
Procedure: Inspect and Clean the Reusable Air Filter

Step 1 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that may have collected on the filter and proceed to Step 3. If the filter is installed beneath the fan tray and not in the external filter brackets, open the ONS 15454 door and fold out the retractable handles at each outside edge of the fan tray.

Step 2 Slide the fan-tray assembly out of the shelf assembly by gently pulling the handles.

Step 3 Visually inspect the air filter material for dirt and dust.

Step 4 If the reusable air filter contains a concentration of dirt and dust, either vacuum the filter or wash the filter under a faucet with a light detergent.

Note If possible, cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 5   If you washed the filter, allow it to completely air dry for at least eight hours and install a spare filter (spare filters should be kept in stock) in its place:

⚠️

Warning   **Do not put a damp filter back in the ONS 15454.**

   a. If the air filter is installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

   b. If the filter is installed beneath the fan-tray assembly, slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment.

Step 6   Push the fan tray back into the shelf assembly.

⚠️

Caution   If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

✎

Note   On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 7   Rotate the retractable handles back into their compartments and close the ONS 15454 front door.

3.1.2 Disposable Air Filter

Versions prior to the NEBS 3E version of the ONS 15454 use a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. This disposable filter is not designed to be cleaned. You can order air filter replacements from Cisco (Cisco P/N 47-01-00001) or from Universal Air Filter, model PE-5 (Universal Air Filter Co., 1624 Sauget Ind. Parkway, Sauget, IL 62206).

✎

Note   The disposable air filter is installed beneath the fan-tray assembly, so you must remove the fan-tray assembly to inspect and replace the disposable air filter.

Procedure: Inspect and Replace the Disposable Air Filter

Step 1   Remove the front door of the shelf assembly.

Step 2   Open the front covers of the fiber management area.

Step 3   Lower the hinged panels in front of the cable management tray.

Step 4   Slide the fan-tray assembly out of the shelf assembly (see Figure 3-2).

Figure 3-2   Inserting or removing the fan-tray assembly

Fan tray
assembly

Fan tray filter

Small engraved
direction arrow

34510
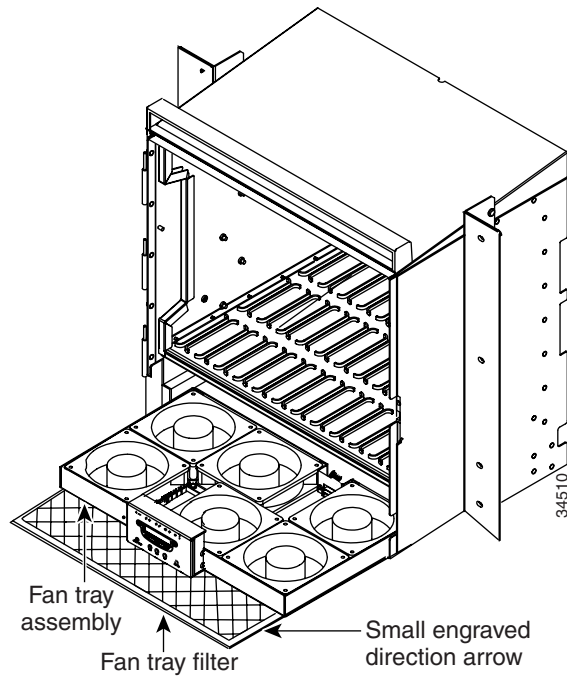
Step 5   Carefully slide the air filter out of the shelf assembly (see Figure 3-3). Be careful not to dislodge any dust that may have collected on the filter.

Step 6   Visually inspect the white filter material for dirt and dust.

Step 7   If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter by sliding the new filter into the bottom of the shelf assembly. Make sure that the front of the filter is flush with the front of the shelf assembly and that the air flow indicators on the filter point upwards.

Figure 3-3   Inserting or removing a disposable fan-tray air filter

Fan tray filter
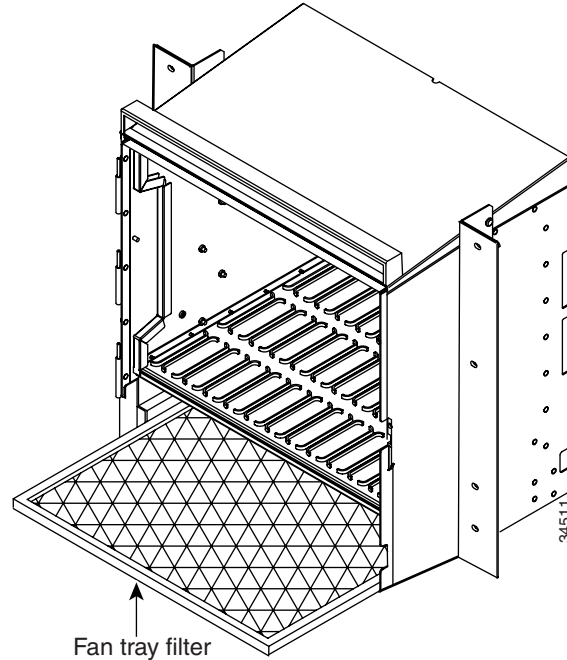
Step 8   Slide the fan-tray assembly into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 9   To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated.

Step 10   Close the cable management tray.

Step 11   Raise the hinged panel at the front of the cable management tray.

Step 12   Close the front covers of the fiber management area.

Step 13   Replace the front door of the shelf assembly.

3.2 Fan-Tray Assembly Replacement

If one or more fans fail on the fan-tray assembly, replace the entire assembly. You cannot replace individual fans. The red Fan Fail LED on the front of the fan tray illuminates when one or more fans fail. The red Fan Fail LED clears after you install a working fan tray.

⚠

Caution   The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.

Note The 10-Gbps compatible shelf assembly (15454-SA-ANSI) and fan-tray assembly (15454-FTA3) are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

Procedure: Replace the Fan-Tray Assembly

To replace the fan-tray assembly, 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.

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.

Step 1 Remove the front door of the shelf assembly.

Step 2 Fold out the retractable handles at the outside edges of the fan tray.

Step 3 Slide the fan tray out of the shelf assembly by gently pulling on the handles. Figure 3-4 shows the location of the fan tray.

Step 4 If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime.

Note The air filter will function with either side facing up but Cisco recommends that you install the filter with the metal bracing facing up against the fan tray.

For more information on the fan-tray air filter, see the "Air Filter Inspection and Replacement" section on page 3-1.

Step 5 Slide the fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 6 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Figure 3-4   Removing or replacing the fan-tray assembly

Fan-tray
assembly
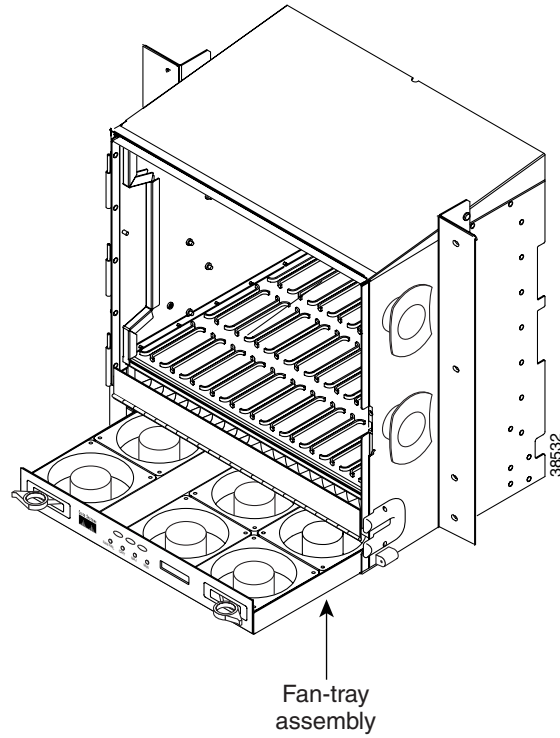
3.3 Alarm Interface Panel Replacement

3.4 Replace the Alarm Interface Panel

This procedure replaces an existing AIP with a new AIP on an in-service system without affecting traffic. It requires a #2 phillips screw driver.

⚠

Caution   Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.

⚠

Caution   There is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Assistance Center (TAC) at 877-323-7368 when prompted to do so in the procedure.

⚠

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

✎

Note   Perform this procedure in a maintenance window. Resetting the active TCC+ can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC+ will cause a service disruption of 3–5 minutes on all Ethernet traffic due to Spanning Tree Reconvergence.

Step 1   Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

   a.   Log into CTC.

   b.   In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.

   c.   If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.

Step 2   Record the MAC address of the old AIP:

   a.   Log into the node where you will replace the AIP. For login procedures, see the Cisco ONS 15454 Procedure Guide.

   b.   In node view, click on the **Provisioning > Network** tabs.

   c.   Record the MAC address shown in the General tab in Figure 3-5.

Figure 3-5   Find the MAC address
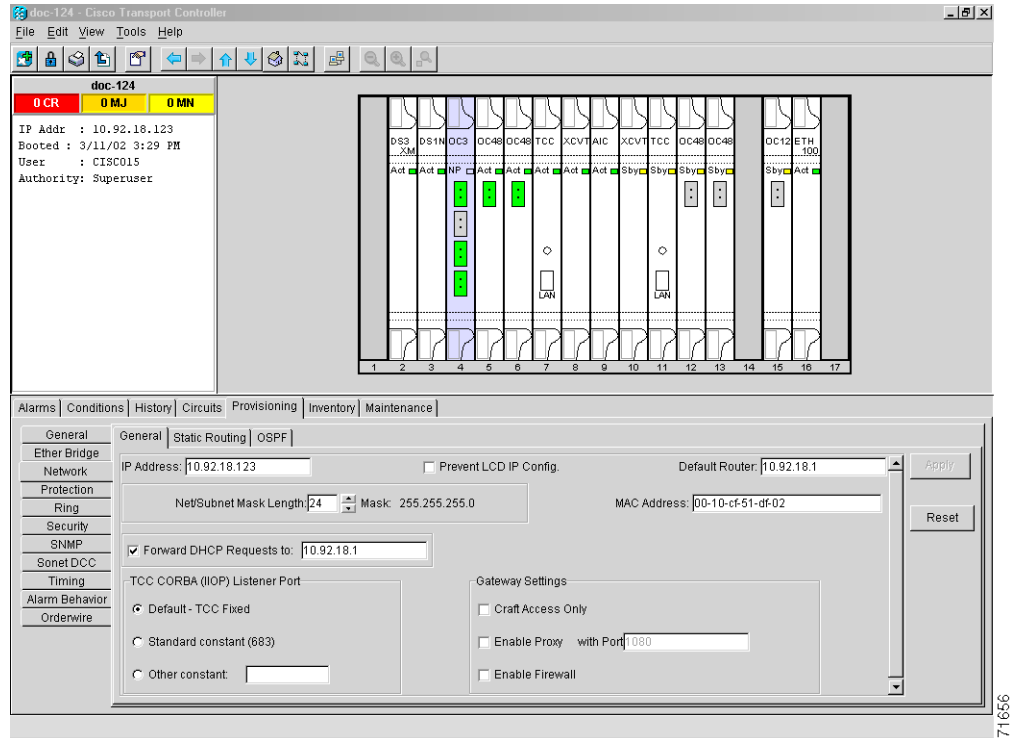
Step 3   Call Cisco TAC at 877-323-7368 for assistance in replacing the AIP and maintaining the original MAC address.

Step 4   Unscrew the five screws that hold the lower backplane cover in place (Figure 3-6).

Step 5   Grip the lower backplane cover and gently pull away from the backplane.

Figure 3-6   Lower backplane cover

Retaining
screws
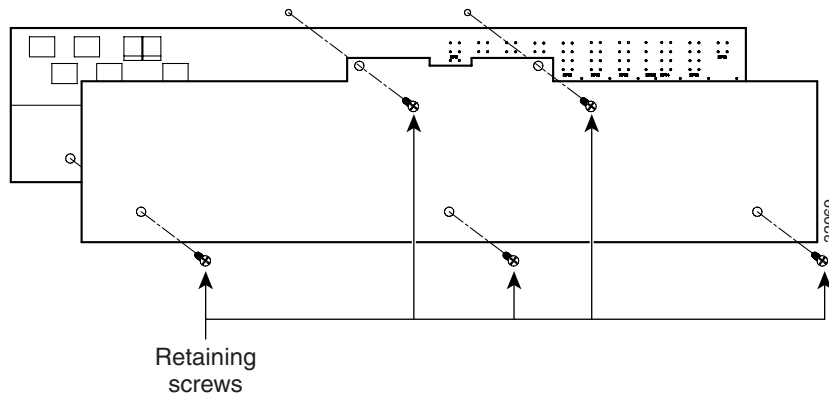
Step 6   Unscrew the two screws that hold the AIP cover in place.

Step 7   Grip the cover and gently pull away from the backplane.

✎
Note   On the 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8   Grip the AIP and gently pull away from the backplane.

Step 9   Disconnect the fan-tray assembly power cable from the AIP.

Step 10   Set the old AIP aside for return to Cisco.

⚠
Caution   The type of shelf the AIP resides in will determine the version of AIP that will replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) currently uses the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and lower currently use the 2A AIP (P/N: 73-5262-01).

⚠
Caution   Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857); doing so will cause a blown fuse on the AIP.

Step 11   Attach the fan-tray assembly power cable to the new AIP.

Step 12   Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13   Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14   Replace the lower backplane cover and secure the cover with the five screws.

Step 15   In node view, click on the **Provisioning > Network** tabs.

⚠
Caution   Cisco recommends TCC+ resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16   Reset the standby TCC+:

    a.   In node view, right click on the standby TCC+ card and choose **Reset Card**.

    b.   Click **Yes** on the Resetting Card dialog box. As the card resets, a loading (Ldg) indication will appear on the card in CTC.

✎
Note   The reset will take approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17   Reset the active TCC+:

    a.   In node view, right click on the active TCC+ card and choose **Reset Card**.

    b.   Click **Yes** on the Resetting Card dialog box. As the card resets, a Ldg indication will appear on the card in CTC.

✎
Note   The reset will take approximately five minutes and CTC will lose its session with the node.

Step 18   Click **File** from the menu bar and choose **Exit** to exit the CTC session.

Step 19 Login back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes pull-down menu.

Step 20 Record the new MAC address:

   a. In node view, click on the **Provisioning > Network** tabs.

   b. Record the MAC address shown in the General tab.

Step 21 In node view, click on the **Circuits** tab. Note that all circuits listed are in an INCOMPLETE state.

Step 22 In node view, choose **Tools** from the menu bar and click **Repair Circuits** (Figure 3-7). The Circuit Repair dialog box is displayed.

Figure 3-7   Repair Circuits in the Menu Bar
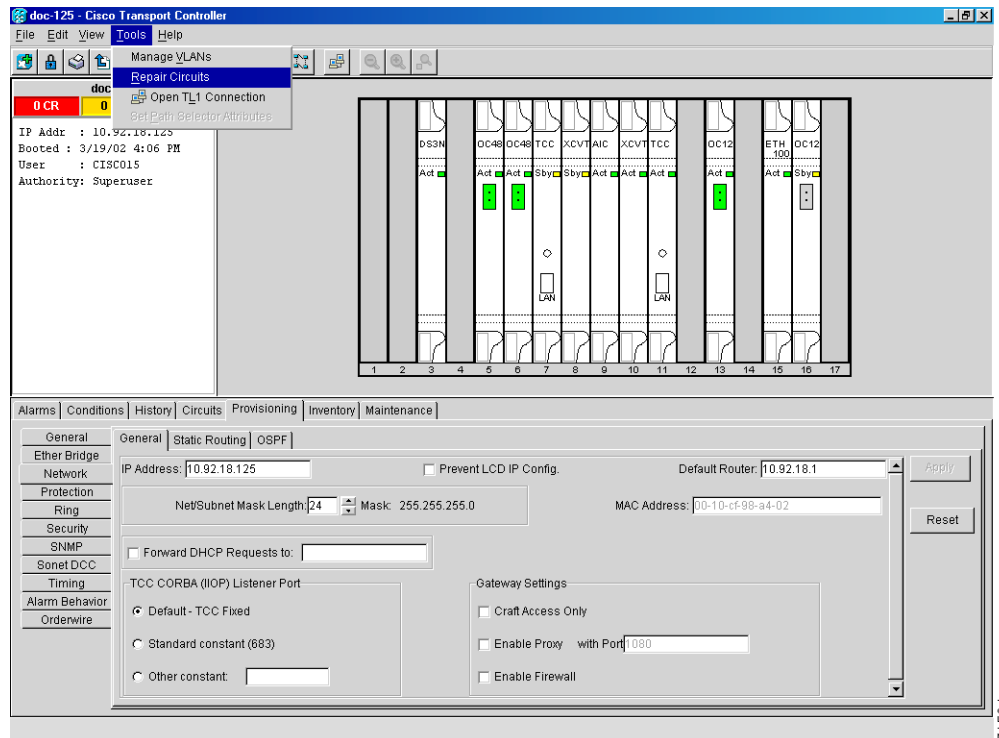
Step 23 Read the instructions in the Circuit Repair dialog box (Figure 3-8). If all the steps in the dialog box have been completed, click **Next>**. Ensure you have the old and new MAC addresses.

Figure 3-8   Repairing circuits
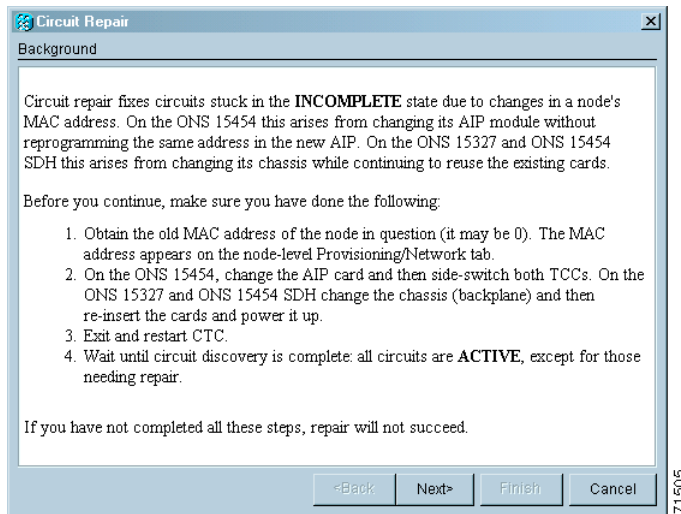
Step 24   The Node MAC Addresses dialog box displays (Figure 3-9):

   a.   From the Node pull down menu, choose the name of the node where you replaced the AIP.

   b.   In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.

   c.   Click **Next**.

Figure 3-9   Recording the old MAC address before replacing the AIP
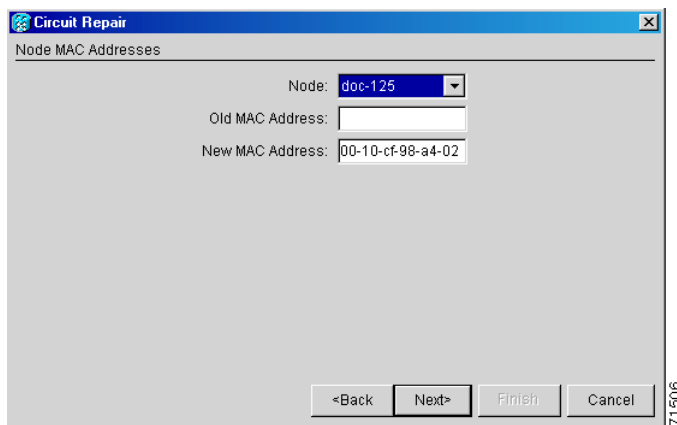
Step 25   The Repair Circuits dialog box displays (Figure 3-10). Read the information in the dialog box and click **Finish**.

Figure 3-10   Circuit repair information
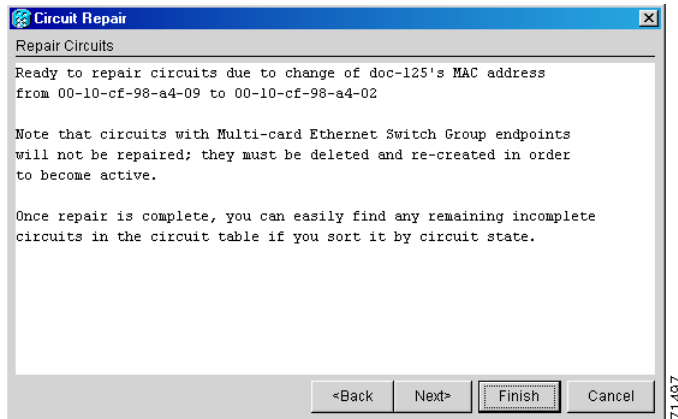
> **Note**   The CTC session will freeze until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

Step 26   When the circuit repair is complete, the Circuits Repaired dialog box will display.

Step 27   Click **OK**.

Step 28   In the new node view, click on the **Circuits** tab. Note that all circuits listed are in an ACTIVE state. If all circuits listed are not in an ACTIVE state, call Cisco TAC at 877-323-7368 for assistance.

Step 29   Return the defective AIP. You must follow the standard Return Material Authorizations (RMA) procedures; call (800) 553-NETS (6387) if you do not have an RMA number.

3.5 System Reset

You can reset the ONS 15454 TCC+ cards by using the Cisco Transport Controller (CTC) software, or by physically reseating a TCC+ card (card pull). A software-initiated reset reboots the TCC+ and reloads the operating system and the application software. Additionally, a card pull reset temporarily removes power from the TCC+ and clears all buffer memory.

You can apply a software-initiated reset to either an active or standby TCC+ without affecting traffic, but you should only perform a card pull on a standby TCC+. If you need to perform a card pull on an active TCC+, put the TCC+ into standby mode first by performing a software-initiated reset on the card.

> **Note**   When a software-initiated reset is performed on an active TCC card or TCC+, the AIC card goes through an initialization process and also resets. The AIC card reset is normal and will happen each time an active TCC card goes through a software-initiated reset.

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

Procedure: Perform a Software-Initiated Reset

Step 1 Log into CTC.

Step 2 Right click on the TCC+ card to reveal a pull-down menu.

Step 3 Click **Reset Card** (see Figure 3-11).

Step 4 Click **Yes** when the "Are You Sure?" dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Step 6 Confirm that the TCC+ is in standby mode after the reset.

Figure 3-11   Performing a software-initiated reset from the TCC+ card pull-down menu
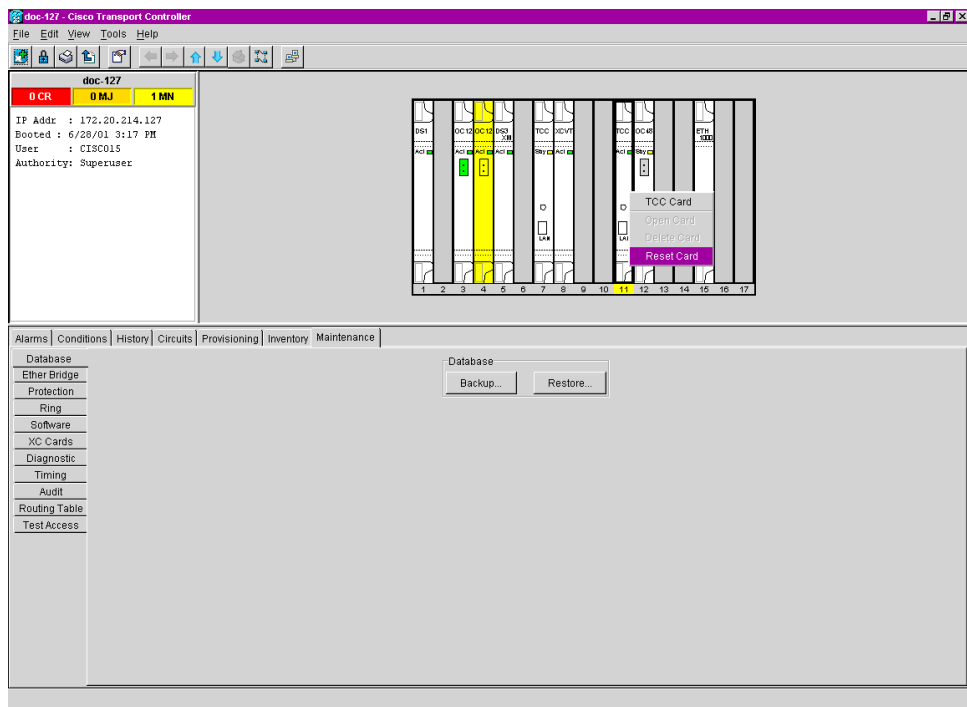
Procedure: Perform a Card Pull

Note To determine whether you have an active or standby TCC+, position the cursor over the TCC+ card graphic to display the status.

Step 1 If you need to perform a card pull on an active TCC+ card, first perform a software-initiated reset on the active TCC+ (see the "Perform a Software-Initiated Reset" procedure on page 3-14).

Step 2 When the TCC+ is in standby mode, unlatch both the top and bottom ejector levers on the TCC+ card.

Step 3 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 4   Wait 30 seconds. Reinsert the card and close the ejector levers.

> ✎
> **Note**   The TCC+ will take several minutes to reboot and will display the amber standby LED after rebooting.

3.6 Database Backup and Restore

Each TCC+ card installed in the ONS 15454 contains two copies of the database. A save to the flash memory is written to the standby database, and the standby database then becomes the active database. The previously active database then becomes available for writing the next time. With dual TCC+s, the standby TCC+ keeps both copies of the database synchronized with the active TCC+ as changes are made so that it is ready to take over control as needed. You can also store a back-up version of the database on the workstation running CTC. Backing up the database should be part of a regular ONS 15454 maintenance program at approximately weekly intervals and should also be completed when preparing an ONS 15454 for a pending natural disaster, such as a flood or fire.

> ✎
> **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.

> ⚠
> **Caution**   E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm will appear and clear during this period.

> ⚠
> **Caution**   If you are restoring the database on multiple nodes, wait five minutes between each database restore.

Procedure: Back up the Database

Step 1   Log into CTC.

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

Figure 3-12   Backing up the TCC+ database
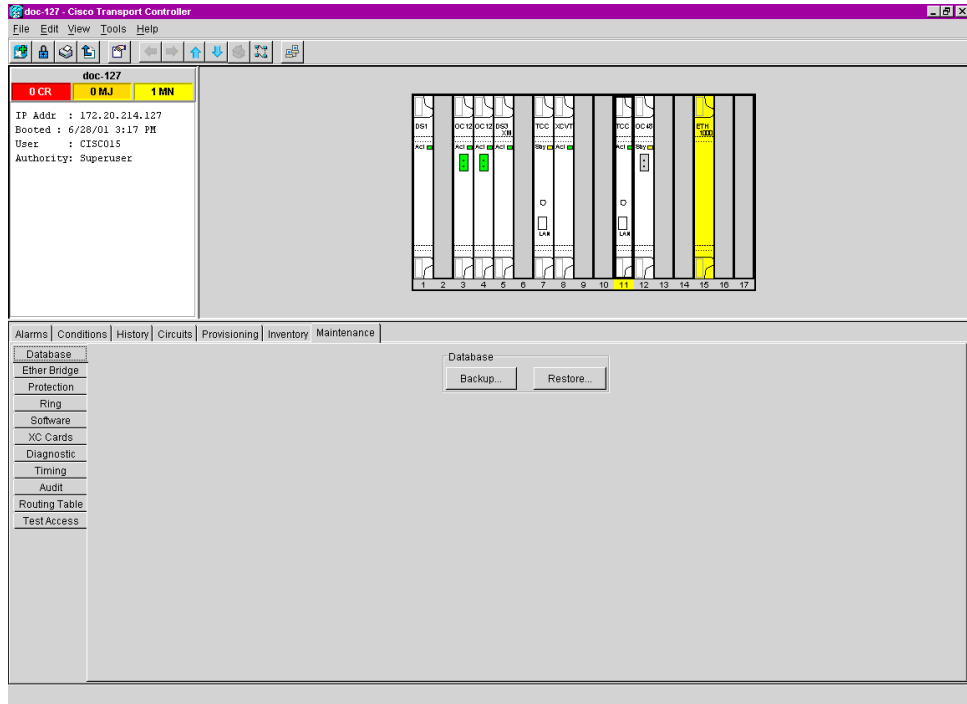
Step 3   Click **Backup**.

Step 4   Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the .db file extension, for example, database.db.

Step 5   Click **Save**.

Figure 3-13   Confirming a database backup
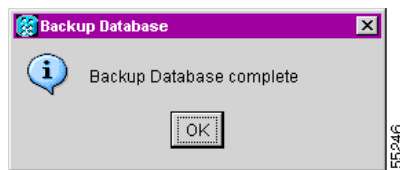
Step 6   Click **OK** in the confirmation dialog box.

Procedure: Restore the Database

Step 1   Log into CTC.

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

Figure 3-14   Restoring the TCC+ database
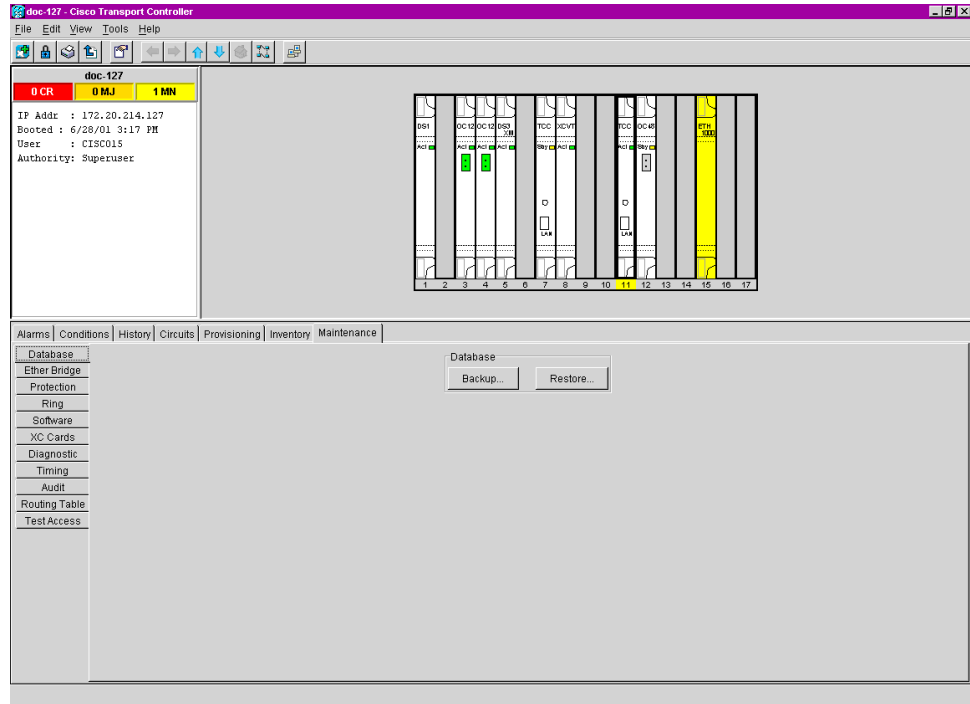
Step 3   Click **Restore**.

Step 4   Locate the database file stored on the workstation's hard drive or on network storage.

Step 5   Click the database file to highlight it.

Step 6   Click **Open**.

The DB Restore dialog box appears. A restore from another node will affect traffic.

Figure 3-15   Restoring the database—traffic loss warning
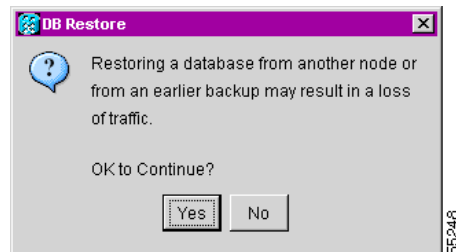
Step 7   Click **Yes**.

The Restore Database dialog box monitors the file transfer.

Figure 3-16   Restoring the database – in-process notification
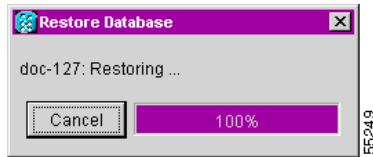
Step 8   Wait for the file to complete the transfer to the TCC+.

Step 9   Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears. Wait for the node to reconnect.

3.7 Reverting to an Earlier Software Load

Prior to Release 2.2.1, the ONS 15454 could not revert to an earlier software database without deleting the current database and losing both cross-connect and DCC connectivity. The revert would result in a loss of traffic until the user manually restored the previous database or recreated the existing circuits and provisioning.

Reverting to a 2.2.1 or later load will switch to the older software load and its attendant database without affecting traffic or DCC connectivity. This feature requires dual TCC+ cards and CTC software Release 2.2.1 or later as the protect version.

When you click the Activate button after a software upgrade, the TCC+ copies the current working database and saves it in a reserved location in the TCC+ flash memory. If you later need to revert to the original working software load from the protect software load, the saved database installs automatically. You do not need to restore the database manually or recreate circuits.

Tip   The revert feature is useful if a maintenance window closes while you are upgrading CTC software. You can revert to the standby software load without losing traffic. When the next maintenance window opens, complete the upgrade and activate the new software load.

Note   A revert to a maintenance release software load does not restore the database and no provisioning is lost. All other reverts do restore the database. (A maintenance release has a three-digit release number, e.g. 2.2.2).

Note   Circuits created and provisioning performed after a software load is activated will not reinstate with a revert. The database configuration at the time of activation is reinstated after a revert. This note does not apply to maintenance reverts (e.g. 2.2.2 to 2.2.1).

Procedure: Revert to an Earlier Software Load

Step 1   Log into CTC.

Step 2   Record the IP address of that node.

Step 3	Display the CTC node view.
Step 4	Right click the standby TCC+ card to reveal a pull-down menu.
Step 5	Click **Reset Card**.
Step 6	Click **Yes** when the "Are You Sure?" dialog box appears.
Step 7	Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.
Step 8	Confirm that the TCC+ is in standby mode after the reset.
Step 9	Click the **Maintenance > Software** tabs.
Step 10	Verify that the protect software is Version 2.2.0 or later.
Step 11	Click **Revert**.
	The Revert button activates the protect software load. The ONS 15454 reboots and loses the connection to CTC.
Step 12	Wait until the software upgrade finishes.
	This may take as long as 30 minutes.
Step 13	Completely close the browser.
Step 14	Restart the browser and log back into the node using the IP address recorded in Step 2.
	The browser downloads the CTC applet for the standby software load.

3.8 Card Replacement

To replace an ONS 15454 card with another card of the same type, you do not need to make any changes to the database; remove the old card and replace it with a new card. To replace a card with a card of a different type, physically remove the card and replace it with the new card, then delete the original card from CTC. Follow the "Switch Traffic and Replace an In-Service Cross-Connect Card" procedure on page 3-20 to replace an XC/XCVT card.

Caution Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, switch it to standby prior to removing the card from the node.

Note An improper removal (IMPROPRMVL) alarm is raised whenever a card pull is performed, unless the card is deleted in CTC first. The alarm will clear after the card replacement is complete.

Note In a UPSR, pulling the active XC/XCVT/XC10G without a lockout will cause UPSR circuits to switch.

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

To upgrade cards, refer to the specific upgrade procedure you need:

- "TCC Card to TCC+ Card Upgrade" section on page 3-21
- "XC Card to XCVT Card Upgrade" section on page 3-22
- "XC/XCVT Card to XC10G Card Upgrade" section on page 3-24
- "DS3/DS3N Card to DS3E/DS3EN Card Upgrade" section on page 3-25

For more information on cards and card compatibility see Chapter 4, "Card Reference."

Procedure: Switch Traffic and Replace an In-Service Cross-Connect Card

⚠

Caution   Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, follow the steps below to switch the XC/XCVT card to standby prior to removing the card from the node.

An XC/XCVT reset can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

Step 1   Take the following precautions before performing an XC/XCVT reset to avoid causing a linear 1+1 or BLSR protection switch:

a.   Ensure the working span is active on both the local and remote nodes.

b.   Ensure the working span is carrying error-free traffic (no SD or SF alarms present).

c.   Lockout the protection span prior to initiating an XC/XCVT reset.

In a BLSR, place a lockout on the East and West cards of the nodes adjacent to the XC/XCVT switch node; for example, to switch the XC/XCVT 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. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.

<------East [Node A] West------East [Node B] West------East [Node C] West------>

In a 1+1 protection scheme, place a lockout on the protect card and verify that the traffic is traveling over the working span before setting the lockout.

Step 2   Determine the active XC/XCVT card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

✎

Note   You can also place the cursor over the card graphic to display a pop-up identifying the card as active or standby.

Step 3   Switch the active XC/XCVT card to standby:

a.   In the node view, click the **Maintenance > XC Cards** tabs.

b.   Under Cross Connect Cards, choose **Switch**.

c.   Click **Yes** on the Confirm Switch dialog box.

✎

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

Step 4   Physically remove the new standby XC/XCVT card from the ONS 15454.

Step 5   Insert the replacement XC/XCVT card into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

Step 6   Release the protection lockout(s).

3.9 TCC Card to TCC+ Card Upgrade

⚠

Caution   The ONS 15454 Release 3.1 must operate with a matching pair of TCC+ cards.

The TCC card supports ONS 15454 Release 2.2.2 and earlier software versions. The TCC+ card supports ONS 15454 Release 2.2.0 and later software versions.

Verify that the ONS 15454 is running Release 2.2.0 software before you begin the upgrade procedure. The TCC to TCC+ upgrade process requires Release 2.2.0 to support the TCC/TCC+ mismatch that occurs briefly during the TCC to TCC+ upgrade process.

The ACT/STBY LED on the faceplate of the TCC/TCC+ card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a standby card. See Chapter 5 for more information about the TCC/TCC+ card.

Procedure: Upgrade the TCC Card to the TCC+ Card

Step 1   Physically replace the standby TCC card on the ONS 15454 with a TCC+ card.

   a.   Open the TCC card ejectors.

   b.   Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.

   c.   Open the ejectors on the TCC+ card.

   d.   Slide the TCC+ card into the slot along the guide rails.

   e.   Close the ejectors.

✎

Note   The MEA (card mismatch) alarm appears because CTC recognizes a mismatch between TCC card types. Disregard this alarm; it clears by the end of the procedure.

✎

Note   It takes approximately 20 or 30 minutes for the active TCC to transfer the system software to the newly-installed TCC+. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the LEDs on the TCC+ flash Fail and then the active/standby LED flashes. When the transfer completes, the TCC+ reboots and goes into standby mode after approximately three minutes.

Step 2   Right click the active TCC card to reveal a pull-down menu.

Step 3   Click **Reset Card** (Figure 3-17).

Figure 3-17   Initiating a software reset on the TCC card
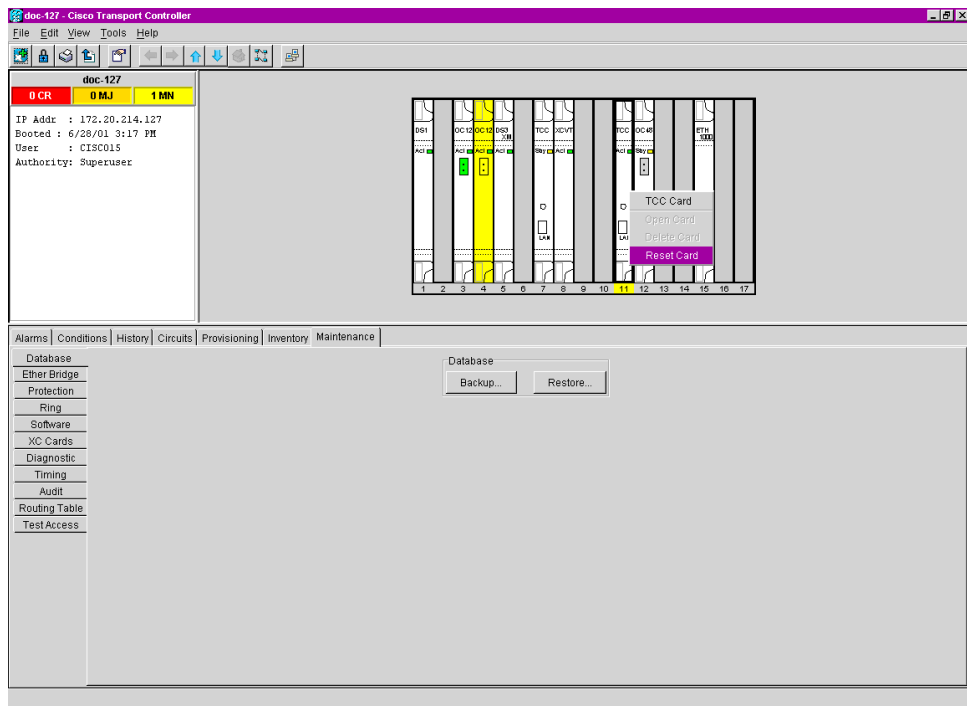
Wait for the TCC to reboot. The ONS 15454 switches the standby TCC+ card to active mode.

Step 4   Verify that the remaining TCC card is now in standby mode (the ACT/STBY LED changes to amber).

Step 5   Physically replace the remaining TCC card with the second TCC+ card.

   a.   Open the TCC card ejectors.

   b.   Slide the card out of the slot.

   c.   Open the ejectors on the TCC+ card.

   d.   Slide the TCC+ card into the slot along the guide rails.

   e.   Close the ejectors.

The ONS 15454 boots up the second TCC+ card. The second TCC+ must also copy the system software, which can take up to 20 or 30 minutes. The MEA alarm clears when the ONS 15454 recognizes the matching TCC+s.

3.10 XC Card to XCVT Card Upgrade

This section explains how to replace dual XC cards with dual XCVT cards in an ONS 15454 with live traffic. The procedure is non-service affecting, that is, the upgrade will cause a switch less than 50 ms in duration.

Note   The UNEQ-P alarm might be raised during a cross-connect card upgrade if you have E100/E1000 cards in the system. The alarm will appear and clear within a few seconds.

Procedure: Upgrade the XC Card to the XCVT Card

Upgrading XC cards to XCVT requires that the ONS 15454 is running CTC Release 2.0 or later. Two XC cards must be installed in the ONS 15454, and two XCVT cards must be available for installation. An XC switch can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

Step 1   Take the following precautions before performing an XC switch to avoid causing a linear 1+1 or BLSR protection switch:

a.   Ensure the working span is active on both the local and remote nodes.

b.   Ensure the working span is carrying error-free traffic (no SD or SF alarms present).

c.   Lockout the protection span prior to initiating an XC reset.

In a BLSR, place a lockout on the East and West cards of the nodes adjacent to the XC switch node; for example, to switch the XC 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. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.

<------East [Node A] West------East [Node B] West------East [Node C] West------>

In a 1+1 protection scheme, place a lockout on the protect card and verify that the traffic is traveling over the working span before setting the lockout.

Step 2   Determine the standby XC card. The ACT/STBY LED of the standby XC card is amber, while the ACT/STBY LED of the active XC card is green.

Note   You can also place the cursor on the card graphic in CTC to display a dialog. This display identifies the card as XC: Active or XC: Standby.

Step 3   Physically replace the standby XC card on the ONS 15454 with an XCVT card:

a.   Open the XC card ejectors.

b.   Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

c.   Open the ejectors on the XCVT card.

d.   Slide the XCVT card into the slot along the guide rails.

The fail LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The ACT/STBY LED turns amber and stays lit.

e.   Close the ejectors.

Step 4   In node view, choose the **Maintenance > XC Cards** tabs.

Step 5   From the Cross Connect Cards menu, choose **Switch**.

Step 6   Click **Yes** on the Confirm Switch dialog box.

Note   After the active XC disengages, the standby slot or first XCVT card becomes active. This causes the ACT/STBY LED on the first XCVT card to change from amber to green.

Step 7   Physically remove the now standby XC card from the ONS 15454 and insert the second XCVT card into the empty XC slot:

a.   Open the XC card ejectors.

 b. Slide the card out of the slot.

 c. Open the ejectors on the XCVT.

 d. Slide the XCVT card into the slot along the guide rails.

 e. Close the ejectors.

The upgrade is complete when the second XCVT card boots up and becomes the standby XCVT.

Step 8 Release the protection lockout.

3.11 XC/XCVT Card to XC10G Card Upgrade

Note This procedure only applies to XC/XCVT cards that are installed in the 15454-SA-ANSI (Release 3.1 or later). You cannot perform this upgrade from shelves released prior to 3.1. The XC10G requires the 15454-SA-ANSI.

Note The UNEQ-P alarm might be raised during a cross-connect card upgrade if you have E100/E1000 cards in the system. The alarm will appear and clear within a few seconds.

This section explains how to upgrade dual XC/XCVT cards with dual XC10G cards in the ONS 15454-SA-ANSI with live traffic. The procedure is non-service affecting, that is, the upgrade will cause a switch less than 50 ms in duration.

Procedure: Upgrade the XC/XCVT Card to the XC10G Card

Upgrading XC/XCVT cards to XC10G requires that the ONS 15454 is running CTC Release 3.1 or later. Two XC/XCVT cards must be installed in the ONS 15454-SA-ANSI, and two XC10G cards must be available for installation. An XC/XCVT switch can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

Step 1 Take the following precautions before performing an XC/XCVT switch to avoid causing a linear 1+1 or BLSR protection switch:

 a. Ensure the working span is active on both the local and remote nodes.

 b. Ensure the working span is carrying error-free traffic (no SD or SF alarms present).

 c. Lockout the protection span prior to initiating an XC/XCVT reset.

   In a BLSR, place a lockout on the East and West cards of the nodes adjacent to the XC/XCVT switch node; for example, to switch the XC/XCVT 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. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.

   <------East [Node A] West------East [Node B] West------East [Node C] West------>

   In a 1+1 protection scheme, place a lockout on the protect card and verify that the traffic is traveling over the working span before setting the lockout.

Step 2   Determine the standby XC/XCVT card. The ACT/STBY LED of the standby XC/XCVT card is amber, while the ACT/STBY LED of the active XC/XCVT card is green.

> **Note**   You can also place the cursor on the card graphic in CTC to display a dialog. This display identifies the card as XC/XCVT: Active or XC/XCVT: Standby.

Step 3   Physically replace the standby XC/XCVT card on the ONS 15454 with an XC10G card:

    a.   Open the XC/XCVT card ejectors.

    b.   Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

    c.   Open the ejectors on the XC10G card.

    d.   Slide the XC10G card into the slot along the guide rails.

       The fail LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The ACT/STBY LED turns amber and stays lit.

    e.   Close the ejectors.

Step 4   In node view, choose the **Maintenance > XC Cards** tabs.

Step 5   From the Cross Connect Cards menu, choose **Switch**.

Step 6   Click **Yes** on the Confirm Switch dialog box.

> **Note**   After the active XC/XCVT disengages, the standby slot or first XC10G card becomes active. This causes the ACT/STBY LED on the first XC10G card to change from amber to green.

Step 7   Physically remove the now standby XC/XCVT card from the ONS 15454 and insert the second XC10G card into the empty XC/XCVT slot:

    a.   Open the XC/XCVT card ejectors.

    b.   Slide the card out of the slot.

    c.   Open the ejectors on the XC10G.

    d.   Slide the XC10G card into the slot along the guide rails.

    e.   Close the ejectors.

    The upgrade is complete when the second XC10G card boots up and becomes the standby XC10G.

Step 8   Release the protection lockout.

3.12 DS3/DS3N Card to DS3E/DS3EN Card Upgrade

You can perform in-service DS3E upgrades for the following ONS 15454 cards:

- DS3 to a DS3E
- DS3N to a DS3EN

Procedure: Upgrade the DS3 Card to the DS3E Card (or the DS3N Card to the DS3EN Card)

Upgrading to DS3E or DS3EN cards requires that the ONS 15454 is running CTC Release 3.1 or later. Upgrades must be performed between two N-type cards or two non-N-type cards. You cannot upgrade between an N-type card and a non-N-type card. When physically replacing the card, the new card must be in same slot as the old card. The DS3E card upgrade supports 1:1 and 1:N protection schemes. The procedure is non-service affecting, that is, the upgrade will cause a switch less than 50 ms in duration.

> **Note** This procedure can also be used to bring forth the capabilities of a DS3E card that was installed in a chassis prior to having the Release 3.1 software load.

> **Note** Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

> **Note** During the upgrade some minor alarms and conditions will be raised and will clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms. If any Service-Affecting alarms occur, Cisco recommends backing out of the procedure.

Step 1 If the card you are upgrading is unprotected, skip to Step 2. If the card you are upgrading is protected, first lockout the protect card:

> **Note** Traffic will be lost during an upgrade on an unprotected card.

   a. In node view, click the **Maintenance > Protection** tabs.

   b. Under Protection Groups, click on the 1:1 or 1:N protection group (that is, the group supporting the 1:1 or 1:N span cards).

   c. Under Selected Group, click on the protect card.

   d. From Inhibit Switching, click **Lock Out**.

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

Step 2 Physically remove the protect DS3 or the protect DS3N card:

   a. Open the DS3/DS3N card ejectors.

   b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 3 Right click on the protect slot and choose **Change Card** from the pull-down menu.

Step 4 Choose the new card (DS3E or DS3EN) from the *Change to* pull-down menu.

Step 5 Click **OK**.

Step 6 Insert the new DS3E or DS3EN card into the protect slot:

   a. Open the ejectors on the DS3E/DS3EN card.

   b. Slide the DS3E/DS3EN card into the slot along the guide rails.

Step 7 Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby.

Step 8   Remove the lockout on the protect card:

    a.   In node view, click the **Maintenance > Protection** tabs.

    b.   Under Protection Groups, click on the 1:1 or 1:N protection group (that is, the group supporting the 1:1 or 1:N span cards).

    c.   Under Selected Group, click on the protect card.

    d.   From Inhibit Switching, click **Unlock**.

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

Step 9   Repeat the steps above for the working card.

> **Note**   After upgrading from a DS3 to DS3E card, check the DS3E line type is set to the framing type employed by your particular SONET network to take full advantage of the performance monitoring capabilities of the DS3E. At the CTC card level, click the **Provisioning>Line** tabs and check the Line Type column.

Procedure: Downgrade a DS3 or DS3N Card

Downgrading can be performed to back out of an upgrade. All ports must be provisioned as UNFRAMED and not have the Path Trace enabled.

> **Note**   Working cards must be downgraded before protect cards.

The procedure for downgrading is the same as upgrading except you choose DS3 or DS3N from the Change Card pull-down menu. To begin the downgrade, right click on the slot to be downgraded and choose **Change Card** from the pull-down menu as instructed above in Step 4 of the upgrade. Follow the remaining steps of the upgrade until the downgrade is complete.

3.13 Span Upgrades

A span is the optical fiber connection between two ONS 15454 nodes. In a span upgrade, the transmission rate of a span is upgraded from a lower to a higher OC-N signal but all other span configuration attributes remain unchanged. With multiple nodes, a span upgrade is a coordinated series of upgrades on all nodes in the ring or protection group in which traffic carried at a lower OC-N rate is transferred to a higher OC-N. You can perform in-service span upgrades for the following ONS 15454 cards:

- OC-12 to OC-48

- OC-12 to OC-192

- OC-48 to OC-192

Use the XC10G card, the TCC+ card, Software R3.1 or later, and the new 15454-SA-ANSI shelf assembly to enable the OC48 IR/STM16 SH AS 1310, OC48 LR/STM16 LH AS 1550, and the OC192 LR/STM64 LH 1550 cards. See Chapter 4, "Card Reference," for more information on card compatibility.

To perform a span upgrade, the higher-rate optical card must replace the lower-rate card in the same slot. If the upgrade is conducted on spans residing in a BLSR, all spans in the ring must be upgraded. The protection configuration of the original lower-rate optical card (two-fiber BLSR, four-fiber BLSR, UPSR, and 1+1) is retained for the higher-rate optical card.

When performing span upgrades on a large number of nodes, Cisco recommends that you upgrade all spans in a ring consecutively and in the same maintenance window. Until all spans are upgraded, mismatched card types will be present.

Cisco recommends using the Span Upgrade Wizard to perform span upgrades. Although you can also use the manual span upgrade procedures, the manual procedures are mainly provided as error recovery for the wizard. The Span Upgrade Wizard and the Manual Span Upgrade procedures require at least two technicians (one at each end of the span) who can communicate with each other during the upgrade. Upgrading a span is non-service affecting and will cause no more than three switches, each of which is less than 50 ms in duration.

Note   Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note   Span upgrades do not upgrade SONET topologies, for example, a 1+1 group to a two-fiber BLSR. See the *Cisco ONS 15454 Installation and Operations Guide* for topology upgrade procedures.

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

3.13.1 Span Upgrade Wizard

The Span Upgrade Wizard automates all steps in the manual span upgrade procedure (BLSR, UPSR, and 1+1). The wizard can upgrade both lines on one side of a four-fiber BLSR or both lines of a 1+1 group; the wizard upgrades UPSRs and two-fiber BLSRs one line at a time. The Span Upgrade Wizard requires that spans have DCC enabled.

The Span Upgrade Wizard provides no way to back out of an upgrade. In the case of an abnormal error, you must exit the wizard and initiate the manual procedure to either continue with the upgrade or back out of it. To continue with the manual procedure, examine the standing conditions and alarms to identify the stage in which the wizard failure occurred.

Note   The Span Upgrade Wizard only supports OC-N span upgrades. It does not support DS-3 upgrades.

Note   During the upgrade some minor alarms and conditions will be raised and will clear automatically. There should be no service-affecting (SA, Major, or Critical) alarms. If any service-affecting alarms occur, Cisco recommends backing out of the procedure.
BLSR Out of Sync alarms will be raised during span upgrades and will clear when the upgrade of all nodes is complete; a four-node BLSR can take up to five minutes to clear all of the Out of Sync alarms. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

Note   If any of the cross connect cards reboot during the span upgrade, you must manually reset the card once the span upgrade procedure is completed on all the nodes in the ring.

Procedure: Perform a Span Upgrade Using the Span Upgrade Wizard

The following procedure shows the Span Upgrade Wizard upgrading the first line of a two-fiber BLSR from OC-48 to OC-192.

Step 1   Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present:

a. In network view, click on the **Alarms** tab to view a list of current alarms.

b. In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.

Step 2   In network view, right-click the span you want to upgrade.

Step 3   Choose Span Upgrade from the pull-down menu (Figure 3-18).

Figure 3-18   Span pull-down menu
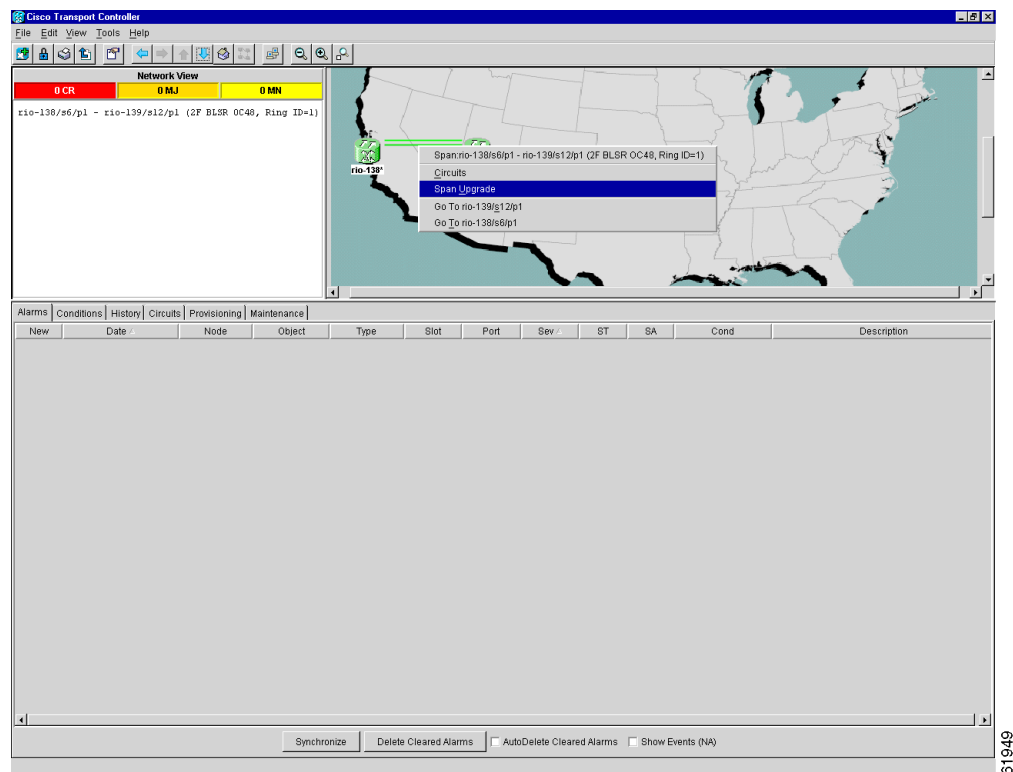
The first Span Upgrade Dialog box appears (Figure 3-19). Follow the instructions on the dialog box and the wizard will lead you through the rest of the span upgrade. The <Back button is only enabled on Step 2 of the wizard; because you cannot back out of an upgrade via the wizard, exit the wizard and initiate the manual procedure if you need to back out of the upgrade at any point beyond Step 2.

Figure 3-19   Beginning the Span Upgrade Wizard
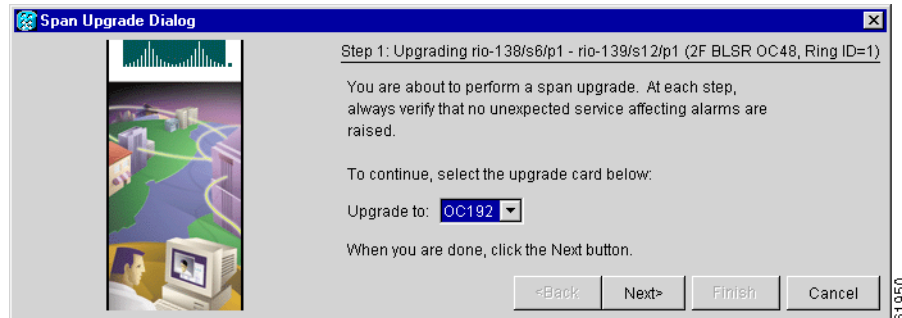
Note   If you install OC-192 cards, an LOS alarm will be reported for each OC-192 slot because the OC-192 laser is disabled. Enable the OC-192 laser by setting the safety key lock to the ON position (1).

Note   Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

3.13.2 Manual Span Upgrades

Manual Span Upgrades are mainly provided as error recovery for the Span Upgrade Wizard, but they can be used to perform span upgrades. Downgrading can be performed to back out of a span upgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card type. You cannot downgrade if circuits exist on the STSs that will be removed (the higher STSs).
Choose from four manual span upgrade options:

- "Perform a Manual Span Upgrade on a Two-Fiber BLSR" procedure on page 3-31
- "Perform a Manual Span Upgrade on a Four-Fiber BLSR" procedure on page 3-32
- "Perform a Manual Span Upgrade on a UPSR" procedure on page 3-33
- "Perform a Manual Span Upgrade on a 1+1 Protection Group" procedure on page 3-34

Note   During the upgrade some minor alarms and conditions will be raised and will clear automatically. There should be no service-affecting (SA, Major, or Critical) alarms. If any service-affecting alarms occur, Cisco recommends backing out of the procedure.
BLSR Out of Sync alarms will be raised during span upgrades and will clear when the upgrade of all nodes is complete. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

> **Note**   If any of the cross connect cards reboot during the span upgrade, you must manually reset the card once the span upgrade procedure is completed on all the nodes in the ring.

Procedure: Perform a Manual Span Upgrade on a Two-Fiber BLSR

All spans connecting the nodes in a BLSR must be upgraded before the added bandwidth is available.

Step 1   Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade:

  a.   In network view, click the **Alarms** tab to view a list of current alarms.

  b.   In network view, click the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.

Step 2   Apply a force switch on the span that you will upgrade first:

  a.   In node view, click the **Maintenance > Ring** tabs.

  b.   Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.

  c.   Click **Apply**.

Step 3   Remove the fiber from both span endpoints (nodes) and ensure that traffic is still running.

Step 4   Remove the OC-N cards from both endpoints.

Step 5   From both endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6   In the Change Card dialog box, choose the new OC-N type.

Step 7   Click **OK**.

Step 8   Install the new OC-N cards in both endpoints and attach the fiber to the cards.

Wait for the IMPROPRMVL alarm to clear and the cards to become active.

> **Note**   If you install OC-192 cards, an LOS alarm will be reported for each OC-192 slot because the OC-192 laser is disabled. Enable the OC-192 laser by setting the safety key lock to the ON position (1).

> **Note**   Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

Step 9   When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:

  a.   In node view, click the **Maintenance > Ring** tabs.

  b.   Click either the West Switch or the East Switch field and choose **CLEAR** from the menu.

  c.   Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

> ✎
> **Note**   You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10   Repeat these steps for each span in the BLSR.
When all spans in the BLSR have been upgraded, the span upgrade is complete.

Procedure: Perform a Manual Span Upgrade on a Four-Fiber BLSR

When upgrading a four-fiber BLSR, you can upgrade both working and protect lines with a single force command. All spans in a BLSR must be upgraded before added bandwidth will be available.

Step 1   Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade:

a.   In network view, click on the **Alarms** tab to view a list of current alarms.

b.   In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.

Step 2   Apply a force switch on the lines that you will upgrade:

a.   In node view, click the **Maintenance > Ring** tabs.

b.   Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.

c.   Click **Apply**.

Step 3   Remove the fiber from both working and protect cards at both span endpoints (nodes) and ensure that traffic is still running.

Step 4   Remove the OC-N cards from both end points.

Step 5   For both ends of the span endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6   In the Change Card dialog box, choose the new OC-N type.

Step 7   Click **OK**.

Step 8   When you have finished Steps 5 through 7 for both nodes, install the new OC-N cards in both endpoints and attach the fiber to the cards.

Wait for the IMPROPRMVL alarm to clear and the cards to become active.

> ✎
> **Note**   If you install OC-192 cards, an LOS alarm will be reported for each OC-192 slot because the OC-192 laser is disabled. Enable the OC-192 laser by setting the safety key lock to the ON position (1).

> ✎
> **Note**   Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

Step 9   When cards on each side of the span have been successfully upgraded and all the facility alarms (LOS, SD, or SF) are cleared, remove the forced switch:

    a. In node view, click the **Maintenance > Ring** tabs.

    b. Click either the West Switch or the East Switch field and choose **CLEAR** from the menu.

    c. Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

> **Note** You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10   Repeat these steps for each span in the BLSR.

When all spans in the BLSR have been upgraded, the span upgrade is complete.

Procedure: Perform a Manual Span Upgrade on a UPSR

Step 1   Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:

    a. In node view, click on the **Alarms** tab to view a list of current alarms.

    b. In node view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.

Step 2   Apply a force switch on the span that you will upgrade:

    a. In network view, right-click the span and choose **Circuits**.

    b. From the Circuits on Span dialog box in the Switch All UPSR Circuits Away field, choose **FORCE**.

    c. Click **Apply**.

Step 3   Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.

Step 4   Remove the OC-N cards from both span endpoints.

Step 5   For both ends of the span, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6   In the Change Card dialog box, choose the new OC-N type.

Step 7   Click **OK**.

Step 8   When you have finished Steps 5 through 7 for both nodes, install the new OC-N cards in both endpoints and attach the fiber to the cards.

Wait for the IMPROPRMVL alarm to clear and the cards to become active.

> **Note** If you install OC-192 cards, an LOS alarm will be reported for each OC-192 slot because the OC-192 laser is disabled. Enable the OC-192 laser by setting the safety key lock to the ON position (1).

> **Note** Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

Step 9 When cards on each side of the span have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:

    a. In network view, right-click the span and choose **Circuits**.

    b. From the Circuits on Span dialog box in the Switch All UPSR Circuits Away field choose **CLEAR**.

    c. Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

> **Note** You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10 The span upgrade is complete.

Procedure: Perform a Manual Span Upgrade on a 1+1 Protection Group

When upgrading a 1+1 group, upgrade the protect line first regardless of which line is active. Both lines in a 1+1 group must be upgraded before the added bandwidth will be available.

> **Note** If the switching mode is bidirectional in the 1+1 protection group, apply the Force command to only one end of the span, not both. The Clear command will apply to the end the Force was applied to. If the Force command is applied to both ends when the switching mode is bidirectional, it will cause a switch of more than 50 ms in duration.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:

    a. In node view, click on the **Alarms** tab to view a list of current alarms.

    b. In node view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.

Step 2 Apply a force switch on the ports that you will upgrade, beginning with the protect port:

    a. In node view, click the **Maintenance > Protection** tabs.

    b. Under Protection Groups, choose the 1+1 protection group.

    c. Under Selected Group, choose the protect port (regardless if it is active or standby).

    d. From Switch Commands, click **Force**.

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

Step 3 Repeat Step 2 for each port.

Step 4 Remove the fiber from both ends of the span and ensure that traffic is still running.

Step 5   Remove the OC-N cards from both span endpoints.

Step 6   At both ends of the span, in node view, right-click the OC-N slot and choose Change Card.

Step 7   In the Change Card dialog box, choose the new OC-N type.

Step 8   Click **OK**.

Step 9   Install the new OC-N cards in both endpoints and attach the fiber to the cards.

Wait for the IMPROPRMVL alarm to clear and the cards to become standby.

> **Note**   If you install OC-192 cards, an LOS alarm will be reported for each OC-192 slot because the OC-192 laser is disabled. Enable the OC-192 laser by setting the safety key lock to the ON position (1).

> **Note**   Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.

Step 10   When cards on each end of the line have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:

   a.   In node view for either endpoint, click the **Maintenance > Protection** tabs.

   b.   Under Protection Groups, choose the 1+1 protection group.

   c.   Under Selected Group, choose the port with the force on it.

   d.   From Switch Commands, click **Clear**.

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

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

> **Note**   You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 11   Repeat these steps for the other line in the 1+1.

When the other line in the 1+1 has been upgraded, the span upgrade is complete.

3.14 Protection Group Switching

Protection group switching allows you to prohibit traffic from switching to a specified card using the Maintenance > Protection tabs. Protection group switching can be accomplished by applying a Lock On or a Lock Out to a specified card. When the Lock On state is applied to a specified working or protect card, any traffic which is currently on that card will remain on that card and will be unable to switch to the opposite card. When the Lock Out state is applied to a specified working or protect card, any traffic which is currently on that card will be switched to the opposite card. A combination of Lock On and Lock Out is allowed in 1:1 and 1:N protection; for example, a Lock On on the working card and a Lock Out on the protect card.

✎
Note   A non-alarmed event (INHSW) is raised when a card is placed in a Lock On or Lock Out state.

Procedure: Apply a Lock On

✎
Note   To apply a Lock On to a protect card in a 1:1 or 1:N protection group, the protect card must be active. If the protect card is not active, the Lock On button is disabled. To make the protect card active, you must switch traffic from the working card to the protect card. When the protect card is active, you can apply the Lock On.

To inhibit traffic from being switched from one card to another, apply a Lock On. Identify which protection group you have to determine which card can be placed in a Lock On state:

- For a 1:1 electrical protection group, both the working and protect cards can be placed in the Lock On state.

- For a 1:N electrical protection group, both the working and protect cards can be placed in the Lock On state.

- For a 1+1 optical protection group, only the working card can be placed in the Lock On state.

Step 1   In Node view, click the **Maintenance > Protection** tabs.

Step 2   Under Protection Groups, click on the protection group you want to switch.

Step 3   Under Selected Group, click on the card you want to lock traffic onto.

Step 4   From Inhibit Switching, click on **Lock On**.

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

The Lock On has been applied and traffic cannot be switched to the opposite card. To clear the Lock On, see the "Clear a Lock On or Lock Out" procedure on page 3-37.

Procedure: Apply a Lock Out

✎
Note   Multiple Lock Outs in the same protection group is not allowed.

To switch traffic from one card to another, apply a Lock Out. Identify which protection group you have to determine which card can be placed in a Lock Out state:

- For a 1:1 electrical protection group, both the working and protect cards can be placed in the Lock Out state.

- For a 1:N electrical protection group, both the working and protect cards can be placed in the Lock Out state.

- For a 1+1 optical protection group, only the protect card can be placed in the Lock Out state.

Step 1   In Node view, click the **Maintenance > Protection** tabs.

Step 2   Under Protection Groups, click on the protection group you want to switch.

Step 3   Under Selected Group, click on the card you want to lock traffic out of.

Step 4   From Inhibit Switching, click on **Lock Out**.

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

The lock out has been applied and traffic is switched to the opposite card. To clear the Lock Out, see the "Clear a Lock On or Lock Out" procedure on page 3-37.

Procedure: Clear a Lock On or Lock Out

Step 1   In Node view, click the **Maintenance > Protection** tabs.

Step 2   Under Selected Group, click on the card you want to clear.

Step 3   From Inhibit Switching, click on **Unlock**.

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

The Lock On or Lock Out is cleared.

3.15 Electrical Interface Assembly Replacement

Electrical interface assemblies (EIAs) provide cable connection points on the back of the ONS 15454 and come in several configurations that work with different cards and connections (see Table 3-1). For more information about EIAs, see the "Installation" chapter of the *Cisco ONS 15454 Installation and Operations Guide*.

EIAs have two sides. As you face the rear of the ONS 15454 shelf assembly, the right-hand side is the A side and the left-hand side is the B side. You can install EIAs on one or both sides of the ONS 15454 backplane in any combination. For example, you can use an AMP Champ EIA on side A and a BNC EIA on side B. The top of the EIA connector columns are labelled with the corresponding slot number, and EIA connector pairs are marked Tx and Rx to correspond to transmit and receive cables. EIAs come pre-installed on the ONS 15454 when ordered with the node.

3.15.1 EIA Types

Table 3-1 gives the product numbers and common names for EIAs.

Table 3-1   EIA Configurations

EIA Type	Cards Supported	A Side Hosts	A Side Columns Map to	A Side Product Number	B Side Hosts	B Side Columns Map to	B Side Product Number
BNC	DS-3 DS3XM-6 EC-1	24 pairs of BNC connectors	Slot 2 Slot 4	15454-EIA-BNC-A24	24 pairs of BNC connectors	Slot 14 Slot 16	15454-EIA-BNC-B24
High-Density BNC	DS-3 DS3XM-6 EC-1	48 pairs of BNC connectors	Slot 1 Slot 2 Slot 4 Slot 5	15454-EIA-BNC-A48	48 pairs of BNC connectors	Slot 13 Slot 14 Slot 16 Slot 17	15454-EIA-BNC-B48
SMB	DS-1 DS-3 EC-1 DS3XM-6	84 pairs of SMB connectors	Slot 1 Slot 2 Slot 3 Slot 4 Slot 5 Slot 6	15454-EIA-SMB-A84	84 pairs of SMB connectors	Slot 12 Slot 13 Slot 14 Slot 15 Slot 16 Slot 17	15454-EIA-SMB-B84
AMP Champ	DS-1	6 AMP Champ connectors	Slot 1 Slot 2 Slot 3 Slot 4 Slot 5 Slot 6	15454-EIA-AMP-A84	6 AMP Champ connectors	Slot 12 Slot 13 Slot 14 Slot 15 Slot 16 Slot 17	15454-EIA-AMP-B84

> **Note**   SMB EIAs support 14 ports per slot when used with a DS-1 card, 12 ports per slot when used with a DS-3 or EC-1 card, and 6 ports per slot when used with a DS3XM-6 card.

3.15.2 EIA Replacement Procedures

The replacement procedure is the same for all the EIA types. However, installing the AMP Champ EIA requires the additional step of attaching the fastening plate to the bottom of the connector row. Before you attach a new EIA, you must remove the backplane cover or EIA already attached to the ONS 15454.

Procedure: Remove the Backplane Cover or EIA

Step 1   To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull the backplane away from the shelf assembly.

Step 2   Loosen the nine perimeter screws that hold the backplane sheet metal cover in place. Do not remove the interior screws.

> **Note**   If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

Step 3   If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.

Step 4   If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull the EIA panel away from the backplane.

> **Note**   Attach backplane sheet metal covers whenever EIAs are not installed.

Procedure: Install the EIAs

Step 1   Line up the connectors on the EIA with the mating connectors on the backplane.

Step 2   Gently push the EIA until both sets of connectors fit together snugly.

Step 3   Replace the nine perimeter screws that you removed while removing the backplane cover.

Step 4   If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

Step 5   Reattach the lower backplane cover.

Due to the large number of BNC connectors on the High-Density BNC EIA, you might require a special tool for inserting and removing BNC EIAs (Figure 3-20). This tool also helps with ONS 15454 patch panel connections.

Figure 3-20   BNC insertion and removal tool
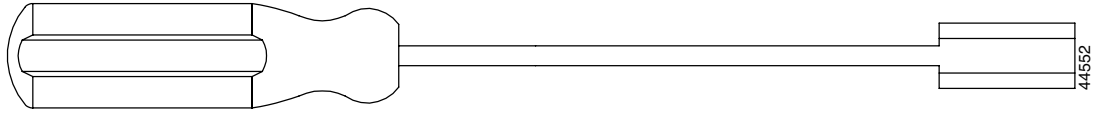
This tool can be obtained with P/N 227-T1000 from:

Amphenol USA (www.amphenol.com)

One Kennedy Drive

Danbury, CT 06810

Phone: 203-743-9272 Fax: 203-796-2032

This tool can be obtained with P/N RT-1L from:

Trompeter Electronics Inc. (www.trompeter.com)

31186 La Baya Drive

Westlake Village, CA 91362-4047

Phone: (800) 982-2629 Fax: (818) 706-1040

3.16 Fiber Cleaning

No special instructions apply to cleaning fibers connected to ONS 15454s. Clean the fiber according to local site practice. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product. An optical fiber maintenance kit can be ordered from Speer Fiber Optics (www.speerfiberoptics.com), part number SFO-1400 NN-A.

3.17 Powering Down a Node

Note   Always use the supplied ESD wristband when working with the Cisco ONS 15454. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf on the NEBS 3 shelf assembly. To access the ESD plug on the NEBS 3 shelf assembly, open the front door of the Cisco ONS 15454. The front door is grounded to prevent electrical shock.

Caution   The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.

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

Procedure: Power Down a Node

Step 1   Identify the node that you want to power down. If no cards are installed, go to Step 12. If cards are installed, log into the node.

Step 2   From the network view, verify that the node is not connected to a working network.

    a.   If the node is part of a working network, log out of the node and follow the procedures to remove a BLSR node or UPSR node in the *Cisco ONS 15454 Installation and Operations Guide, Release 3.2*. Then continue with Step 3.

    b.   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 3–8 are skipped.

Step 3   From the node view, choose 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, as follows:

    a.   Click the circuits that need to be deleted and click **Delete**.

    b.   Click **Yes**.

    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 node view, choose the **Provisioning > SONET DCC** tabs and delete all SDCC terminations.

Step 6   For each installed card, from card view, click the **Provisioning > Line** tabs and place all ports in "Out of Service" mode.

Step 7   Remove all fiber connections to the cards.

Step 8   Right-click on the installed card and click **Delete**.

Step 9   Click **Yes**.

Step 10   After you have deleted the card, open the card ejectors and remove it from the node. Repeat Steps 6–10 for each installed card.

Step 11   Shut off the power from the power supply that feeds the node.

Step 12   Disconnect the node from its external fuse source.

Step 13   Store all cards removed and update inventory records according to local site practice.

4

Card Reference

This chapter describes Cisco ONS 15454 card features and functions. For installation and card turn-up procedures, see the *Cisco ONS 15454 Installation and Operations Guide*.

4.1 Card Overview

The card overview section summarizes card functions, power consumption, temperature ranges, and compatibility.

> **Note**   Each card is marked with a symbol that corresponds to a slot (or slots) on the ONS 15454 shelf assembly. The cards are then installed into slots displaying the same symbols. See the *Cisco ONS 15454 Installation and Operations Guide* for a list of slots and symbols.

4.1.1 Common Control Cards

Table 4-1 lists five common control cards for the Cisco ONS 15454 and summarizes card functions.

Table 4-1   Common Control Card Functions

Card	Description	For Additional Information...
TCC+	The TCC+ is the main processing center for the ONS 15454 and provides system initialization, provisioning, alarm reporting, maintenance, and diagnostics.	See the "Timing Communication and Control (TCC+) Card" section on page 4-16
XC	The XC card is the central element for switching; it establishes connections and performs time division switching (TDS).	See the "XC Cross-Connect Card" section on page 4-19
XCVT	The XCVT card is the central element for switching; it establishes connections and performs time division switching (TDS). The XCVT can manage STS and VT circuits up to 48c.	See the "XCVT Cross-Connect Card" section on page 4-22

Table 4-1   Common Control Card Functions (continued)

Card	Description	For Additional Information...
XC10G	The XC10G card is the central element for switching; it establishes connections and performs time division switching (TDS). The XC10G can manage STS and VT circuits up to 192c. The XC10G allows up to four times the bandwidth of current XC and XCVT cards.	See the "XC10G Cross-Connect Card" section on page 4-26
AIC	The AIC card provides customer-defined alarms with its additional input/output alarm contact closures.	See the "Alarm Interface Controller Card" section on page 4-29

4.1.2 Electrical Cards

Table 4-2 lists the Cisco ONS 15454 electrical cards.

Table 4-2   Electrical Cards for the ONS 15454

Card	Port Description	For Additional Information...
EC1-12	The EC1-12 card provides 12 STS-1 electrical ports.	See the "EC1-12 Card" section on page 4-33
DS1-14	The DS1-14 card provides 14 DS-1 ports.	See the "DS1-14 Card" section on page 4-35
DS1N-14	The DS1N-14 card provides 14 DS-1 ports but can also provide 1:N protection when necessary.	See the "DS1N-14 Card" section on page 4-38
DS3-12	The DS3-12 card has 12 DS-3 ports.	See the "DS3-12 Card" section on page 4-41
DS3N-12	The DS3N-12 card has 12 DS-3 ports but can also provide 1:N protection when necessary.	See the "DS3N-12 Card" section on page 4-44
DS3-12E	The DS3-12E card has 12 ports, supports 1:1 protection, and provides enhanced performance-monitoring functions.	See the "DS3-12E Card" section on page 4-47
DS3N-12E	The DS3N-12E card has 12 ports, supports 1:N protection, and provides enhanced performance-monitoring functions.	See the "DS3N-12E Card" section on page 4-50
DS3XM-6 Transmux	The DS3XM-6 card can convert six framed DS-3 network connections into 168 VT1.5s.	See the "DS3XM-6 Card" section on page 4-53

4.1.3 Optical Cards

Table 4-3 lists the Cisco ONS 15454 optical cards.

Table 4-3   Optical Cards for the ONS 15454

Card	Port Description	For Additional Information...
OC3 IR 4 SH 1310	The OC3 IR 4 1310 card provides four intermediate or short-range OC-3 ports. **Note** The OC3 IR 4 SH 1310 and OC3 IR 4/STM1 SH 1310 cards are functionally the same.	See the "OC3 IR 4/STM1 SH 1310 Card" section on page 4-56
OC12 IR 1310	The OC12 IR 1310 card provides one intermediate or short-range OC-12 port. **Note** The OC12 IR 1310 and OC12/STM4 SH 1310 cards are functionally the same.	See the "OC12 IR/STM4 SH 1310 Card" section on page 4-59
OC12 LR 1310	The OC12 LR 1310 card provides one long-range OC-12 port and operates at 1310 nm. **Note** The OC12 LR 1310 and OC12 LR/STM4 LH 1310 cards are functionally the same.	See the "OC12 LR/STM4 LH 1310 Card" section on page 4-62
OC12 LR 1550	The OC12 LR 1550 card provides one long-range OC-12 port and operates at 1550 nm. **Note** The OC12 LR 1550 and OC12 LR/STM4 LH 1550 cards are functionally the same.	See the "OC12 LR/STM4 LH 1550 Card" section on page 4-65
OC3 IR 4/ STM1 SH 1310	The OC3 IR 4/STM1 SH 1310 card provides four intermediate or short-range OC-3 ports.	See the "OC3 IR 4/STM1 SH 1310 Card" section on page 4-56
OC12 IR/STM4 SH 1310	The OC12 IR/STM4 SH 1310 card provides one intermediate or short-range OC-12 port.	See the "OC12 IR/STM4 SH 1310 Card" section on page 4-59
OC12 LR/ STM4 LH 1310	The OC12 LR/STM4 LH 1310 card provides one long-range OC-12 port and operates at 1310 nm.	See the "OC12 LR/STM4 LH 1310 Card" section on page 4-62
OC12 LR/ STM4 LH 1550	The OC12 LR/STM4 LH 1550 card provides one long-range OC-12 port and operates at 1550 nm.	See the "OC12 LR/STM4 LH 1550 Card" section on page 4-65
OC48 IR 1310	The OC48 IR 1310 card provides one intermediate-range OC-48 port and operates at 1310 nm. This card functions in slots 5, 6, 12, or 13 only.	See the "OC48 IR 1310 Card" section on page 4-68
OC48 LR 1550	The OC48 LR 1550 card provides one long-range OC-48 port and operates at 1550 nm. This card functions in slots 5, 6, 12, or 13 only.	See the "OC48 LR 1550 Card" section on page 4-71
OC48 IR/ STM16 SH AS 1310	The OC48 IR/STM16 SH AS 1310 card provides one intermediate-range OC-48 port and operates in any multispeed or high-speed card slot.	See the "OC48 IR/STM16 SH AS 1310 Card" section on page 4-74
OC48 LR/ STM16 LH AS 1550	The OC48 LR/STM16 LH AS 1550 card provides one long-range OC-48 port and operates in any multispeed or high-speed card slot.	See the "OC48 LR/STM16 LH AS 1550 Card" section on page 4-77
OC48 ELR/ STM16 EH 100 GHz	Thirty-seven distinct OC48 ITU 100 GHz dense wavelength division multiplexing (DWDM) cards provide the ONS 15454 DWDM channel plan.	See the "OC48 ELR/STM16 EH 100 GHz Cards" section on page 4-80

Table 4-3   Optical Cards for the ONS 15454 (continued)

Card	Port Description	For Additional Information...
OC48 ELR 200 GHz	Eighteen distinct OC48 ITU 200GHz DWDM cards provide the ONS 15454 DWDM channel plan.	See the "OC48 ELR 200 GHz Cards" section on page 4-83
OC192 LR/ STM64 LH 1550	The OC192 LR/STM64 LH 1550 card provides one long-range OC-192 port and operates at 1550 nm.	See the "OC192 LR/STM64 LH 1550 Card" section on page 4-87

4.1.4 Ethernet Cards

Table 4-4 lists the Cisco ONS 15454 Ethernet cards.

Table 4-4   Ethernet Cards for the ONS 15454

Card	Port Description	For Additional Information...
E100T-12	The E100T-12 card provides 12 switched, autosensing, 10/100 Base-T Ethernet ports.	See the "E100T-12 Card" section on page 4-90
E1000-2	The E1000-2 card provides two ports of IEEE-compliant, 1000 Mbps ports.	See the "E1000-2 Card" section on page 4-96
E100T-G	The E100T-G card provides 12 switched, autosensing, 10/100 Base-T Ethernet ports and is compatible with the XC10G card.	See the "E100T-G Card" section on page 4-93
E1000-2-G	The E1000-2-G card provides two ports of IEEE-compliant, 1000 Mbps ports and is compatible with the XC10G card.	See the "E1000-2-G Card" section on page 4-99
G1000-4	The G1000-4 card provides four ports of IEEE-compliant, 1000 Mbps ports and is compatible with the XC10G card.	See the "G1000-4 Card" section on page 4-102

4.1.5 Card and Fan-Tray Assembly Power Requirements

Table 4-5 lists power requirements for individual cards and Table 4-6 on page 4-6 shows fan-tray assembly power requirements.

Note Asterisks (*) next to card or fan tray names mean the power specification shown below is based on a calculation because an actual measurement was not available at the time of publication.

Table 4-5   Individual Card Power Requirements

Card Type	Card Name	Watts	Amps	BTU/Hr.
Control Cards	TCC+	9.82	0.20	33.53
	XC *	13	0.28	46
	XCVT	34.40	0.72	117.46
	XC10G *	54	1.12	184.38
	AIC	6.01	0.12	20.52
Electrical Cards	EC1-12	36.60	0.76	124.97
	DS1-14	12.60	0.26	43.02
	DS1N-14	12.60	0.26	43.02
	DS3-12	38.20	0.79	130.43
	DS3N-12	38.20	0.79	130.43
	DS3-12E	26.80	0.56	91.51
	DS3N-12E	26.80	0.56	91.51
	DS3XM-6 Transmux *	20	0.42	68
Optical Cards	OC3 IR 4 SH 1310	19.20	0.40	65.56
	OC12 IR 1310	10.90	0.23	37.22
	OC12 LR 1310	10.90	0.23	37.22
	OC12 LR 1550	9.28	0.19	31.68
	OC3 IR 4/ STM1 SH 1310	19.20	0.40	65.56
	OC12 IR/ STM4 SH 1310	10.90	0.23	37.22
	OC12 LR/ STM4 LH 1310 *	12	0.25	41
	OC12 LR/ STM4 LH 1550	9.28	0.19	31.68
	OC48 IR 1310	32.20	0.67	109.94
	OC48 LR 1550	26.80	0.56	91.50
	OC48 IR/ STM16 SH AS 1310	37.20	0.77	127.01
	OC48 LR/ STM16 LH AS 1550	37.20	0.77	127.01
	OC48 ELR/ STM16 EH 100 GHz	31.20	0.65	106.53
	OC48 ELR 200 GHz	31.20	0.65	106.53
	OC192 LR/ STM64 LH 1550	72.20	1.50	246.52
Ethernet Cards	E100T-12	65	1.35	221.93
	E1000-2	53.50	1.11	182.67
	E100T-G	65	1.35	221.93
	E1000-2-G	53.50	1.11	182.67
	G1000-4	63.00	1.31	215.11

Table 4-6   Fan Tray Assemblies

Fan Tray Assembly	Watts	Amps	BTU/Hr.
FTA2 *	58	1.21	198
FTA3 *	95	1.98	324

4.1.6 Card Temperature Ranges

Table 4-7 shows C-Temp and I-Temp compliant cards and their product names.

Note   The I-Temp symbol is displayed on the faceplate of an I-Temp compliant card. A card without this symbol is C-Temp compliant.

Table 4-7   Card Temperature Ranges and Product Names for the ONS 15454

Card	C-Temp Product Name (0 to +55 degrees Celsius)	I-Temp Product Name (-40 to +65 degrees Celsius)
TCC+	15454-TCC+	15454-TCC+T
XC	15454-XC	15454-XC-T
XCVT	15454-XC-VT	15454-XC-VT-T
XC10G	15454-XC-10G	—
AIC	15454-AIC	15454-AIC-T
EC1-12	15454-EC1-12	15454-EC1-12-T
DS1-14	15454-DS1-14	15454-DS1-14-T
DS1N-14	15454-DS1N-14	15454-DS1N-14-T
DS3-12	15454-DS3-12	15454-DS3-12-T
DS3N-12	15454-DS3N-12	15454-DS3N-12-T
DS3-12E	—	15454-DS3-12E-T
DS3N-12E	—	15454-DS3N-12E-T
DS3XM-6 (Transmux)	15454-DS3XM-6	15454-DS3XM-6-T
OC3 IR 4/STM1 SH 1310	15454-OC34IR1310	15454-OC34I13-T
OC12 IR/STM4 SH 1310	15454-OC121IR1310	15454-OC121I13-T
OC12 LR/STM4 LH 1310	15454-OC121LR1310	15454-OC121L13-T
OC12 LR/STM4 LH 1550	15454-OC121LR1550	15454-OC121L15-T
OC48 IR 1310	15454-OC481IR1310	—
OC48 LR 1550	15454-OC481LR1550	—
OC48 IR/STM16 SH AS 1310	15454-OC481IR1310A	—
OC48 LR/STM16 LH AS 1550	15454-OC481LR1550A	—
OC192 LR/STM64 LH 1550	15454-OC192LR1550	—
E100T-12	15454-E100T	—

Table 4-7   Card Temperature Ranges and Product Names for the ONS 15454 (continued)

Card	C-Temp Product Name (0 to +55 degrees Celsius)	I-Temp Product Name (-40 to +65 degrees Celsius)
E1000-2	15454-E1000-2	—
E100T-G	15454-E100T-G	—
E1000-2-G	15454-E1000-2-G	—
G1000-4	15454-G1000-4	—
OC48 ELR/STM16 EH 100 GHz	15454-OC48E-1-28.7	—
	15454-OC48E-1-30.3	
	15454-OC48E-1-31.1	
	15454-OC48E-1-31.9	
	15454-OC48E-1-32.6	
	15454-OC48E-1-33.4	
	15454-OC48E-1-34.2	
	15454-OC48E-1-35.0	
	15454-OC48E-1-35.8	
	15454-OC48E-1-36.6	
	15454-OC48E-1-38.1	
	15454-OC48E-1-38.9	
	15454-OC48E-1-39.7	
	15454-OC48E-1-40.5	
	15454-OC48E-1-41.3	
	15454-OC48E-1-42.1	
	15454-OC48E-1-42.9	
	15454-OC48E-1-43.7	
	15454-OC48E-1-44.5	
	15454-OC48E-1-46.1	
	15454-OC48E-1-46.9	
	15454-OC48E-1-47.7	
	15454-OC48E-1-48.5	
	15454-OC48E-1-49.3	
	15454-OC48E-1-50.1	

Table 4-7   Card Temperature Ranges and Product Names for the ONS 15454 (continued)

Card	C-Temp Product Name (0 to +55 degrees Celsius)	I-Temp Product Name (-40 to +65 degrees Celsius)
OC48 ELR/STM16 EH 100 GHz (continued)	15454-OC48E-1-50.9	—
	15454-OC48E-1-51.7	
	15454-OC48E-1-52.5	
	15454-OC48E-1-54.1	
	15454-OC48E-1-54.9	
	15454-OC48E-1-55.7	
	15454-OC48E-1-56.5	
	15454-OC48E-1-57.3	
	15454-OC48E-1-58.1	
	15454-OC48E-1-58.9	
	15454-OC48E-1-59.7	
	15454-OC48E-1-60.6	
OC48 ELR/STM16 EH 200 GHz	15454-OC48E-30.33	—
	15454-OC48E-31.90	
	15454-OC48E-33.47	
	15454-OC48E-35.04	
	15454-OC48E-36.61	
	15454-OC48E-38.19	
	15454-OC48E-39.77	
	15454-OC48E-31.35	
	15454-OC48E-42.94	
	15454-OC48E-47.72	
	15454-OC48E-49.32	
	15454-OC48E-50.92	
	15454-OC48E-52.52	
	15454-OC48E-54.13	
	15454-OC48E-55.75	
	15454-OC48E-57.36	
	15454-OC48E-58.98	
	15454-OC48E-60.61	

4.1.7 Card Compatibility

The tables below list ONS 15454 cards, compatible software versions, and compatible cross-connect cards. Read each card description for detailed information about the card. In the tables below, **Yes** means cards are compatible with the listed software versions and cross-connect cards. Table cells with dashes mean cards are not compatible with the listed software versions or cross-connect cards.

Table 4-8   TCC+ Card Software and Cross-Connect Card Compatibility for the ONS 15454

Timing and Control Card	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
TCC+	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4-9   Cross-Connect Card Software and Hardware Compatibility for the ONS 15454

Cross-Connect Cards	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
XC	Yes	Yes	Yes	Yes	Yes	Yes	—
XCVT	Yes	Yes	Yes	Yes	Yes	Yes	—
XC10G	—	—	—	Yes	—	—	Yes, See Note

Note   To enable OC-192 and OC-48 any slot card operation, use the XC10G card, the TCC+ card, Software R3.1 or higher, and the new 15454-SA-ANSI shelf assembly. Do not pair an XC or XCVT with an XC10G.

Table 4-10   Alarm Interface Controller Card Software and Cross-Connect Card Compatibility for the ONS 15454

Alarm Interface Controller Card	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
AIC	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4-11   Electrical Card Software and Cross-Connect Card Compatibility for the ONS 15454

Electrical Cards	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
EC1-12	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DS1-14	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DS1N-14	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DS3-12	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DS3N-12	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DS3-12E	—	See Note	Yes	Yes	Yes	Yes	Yes
DS3N-12E	—	See Note	Yes	Yes	Yes	Yes	Yes

Table 4-11   Electrical Card Software and Cross-Connect Card Compatibility for the ONS 15454 (continued)

Electrical Cards	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
DS3XM-6 (Transmux)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note Use Software R3.0 or higher to enable all enhanced performance monitoring functions on the DS-3E cards. With Software R2.2.2, the DS-3E cards operate as the older DS-3 cards without enhanced performance monitoring.

Table 4-12   Optical Card Software and Cross-Connect Card Compatibility for the ONS 15454

Optical Cards	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
OC3 IR 4 1310	Yes	Yes	Yes	Yes, See Note	Yes	Yes	Yes
OC12 IR 1310	Yes	Yes	Yes	Yes, See Note	Yes	Yes	Yes
OC12 LR 1310	Yes	Yes	Yes	Yes, See Note	Yes	Yes	Yes
OC12 LR 1550	Yes	Yes	Yes	Yes, See Note	Yes	Yes	Yes

Note The OC-3 and OC-12 cards listed above are functionally the same as the equivalent card listed below with the STM-N name.

OC3 IR 4/STM1 SH 1310	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC12 IR/STM4 SH 1310	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC12 LR/STM4 LH 1310	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC12 LR/STM4 LH 1550	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC48 IR 1310	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC48 LR 1550	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC48 IR/STM16 SH AS 1310	—	—	—	Yes, See Note	—	—	Yes, See Note
OC48 LR/STM16 LH AS 1550	—	—	—	Yes, See Note	—	—	Yes, See Note

Note Use the XC10G card, the TCC+ card, Software R3.1 or higher and the new 15454-SA-ANSI shelf assembly to enable the OC48 IR/STM16 SH AS 1310, OC48 LR/STM16 LH AS 1550, and the OC192 LR/STM64 LH 1550 cards.

OC48 ELR/STM16 EH 100 GHz	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC48 ELR 200 GHz	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OC192 LR/STM64 LH 1550	—	—	—	Yes, See Note	—	—	Yes, See Note

Table 4-13   Ethernet Card Software and Cross-Connect Card Compatibility for the ONS 15454

Ethernet Cards	Software R2.2.1	Software R2.2.2	Software R3.0.1	Software R3.1	XC Card	XCVT Card	XC10G Card
Note All cards listed are compatible with Software R3.2.							
E100T-12	Yes	Yes	Yes	Yes	Yes	Yes	—
E1000-2	Yes	Yes	Yes	Yes	Yes	Yes	—
E100T-G	Yes	Yes	Yes	Yes	Yes	Yes	Yes, See Note
E1000-2-G	Yes	Yes	Yes	Yes	Yes	Yes	Yes, See Note
G1000-4	—	—	—	—	—	—	Yes, See Note

Note   To use Ethernet cards with the XC10G, select either the E100T-G card, the E1000-2-G card, or the G1000-4 card. Do not use the E100T-12 card or E1000-2 card with the XC10G. The G1000-4 is not compatible with the XC or XCVT cards.

4.2 Electrical Card Protection

The ONS 15454 provides a variety of electrical card protection methods. This section describes the protection options. Figure 4-1 shows a 1:1 protection scheme and Figure 4-2 on page 4-13 shows a 1:N protection scheme.

4.2.1 Protection, 1:1

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 4-1 shows the ONS 15454 in a 1:1 protection configuration. Each working card in an odd-numbered slot is paired with a protect card in an even-numbered slot: Slot 1 is protecting Slot 2, Slot 3 is protecting Slot 4, Slot 5 is protecting Slot 6, Slot 17 is protecting Slot 16, Slot 15 is protecting Slot 14, and Slot 13 is protecting Slot 12. The following electrical cards use a 1:1 protection scheme: EC1-12, DS1-14, DS3-12 and DS3-12E.

Figure 4-1   ONS 15454 cards in a 1:1 protection configuration
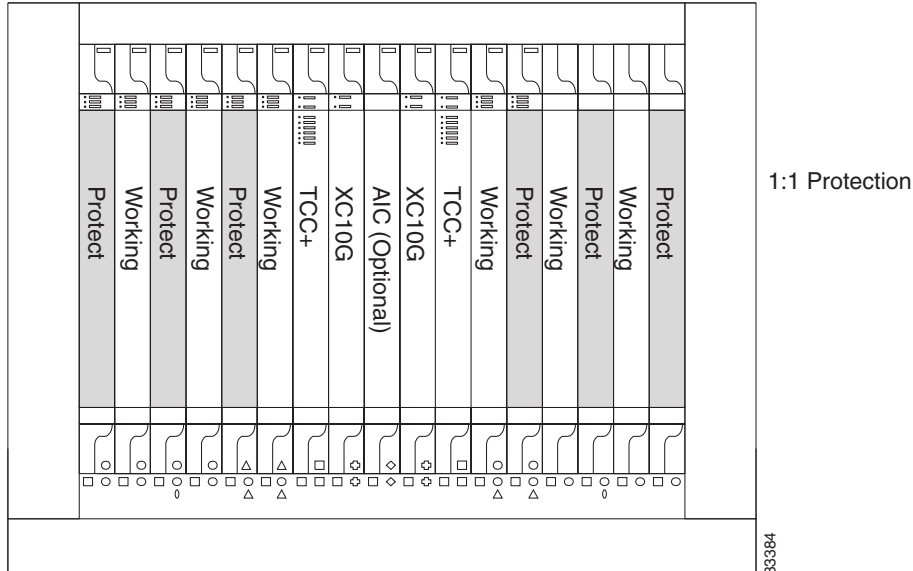
4.2.2 Protection, 1:N

1:N protection allows a single card to protect up to five working cards of the same DS-N level. A DS1N-14 card protects DS1-14 cards, a DS3N-12 card protects DS3-12 cards, and DS3N-12E cards protect DS3-12E cards. The standard DS1-14, DS3-12, and DS3-12E cards provide 1:1 protection only. Currently, 1:N protection operates only at the DS-1 and DS-3 levels. 1:N cards have added circuitry to act as the protection card in a 1:N protection group. Otherwise, the card is identical to the standard card and can serve as a normal working card.

The physical DS-1 or DS-3 interfaces on the ONS 15454 backplane use the working card until the working card fails. When the node detects this failure, the protection card takes over the physical DS-1 or DS-3 electrical interfaces through the relays and signal bridging on the backplane. Figure 4-2 shows the ONS 15454 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 4-2   ONS 15454 cards in a 1:N protection configuration
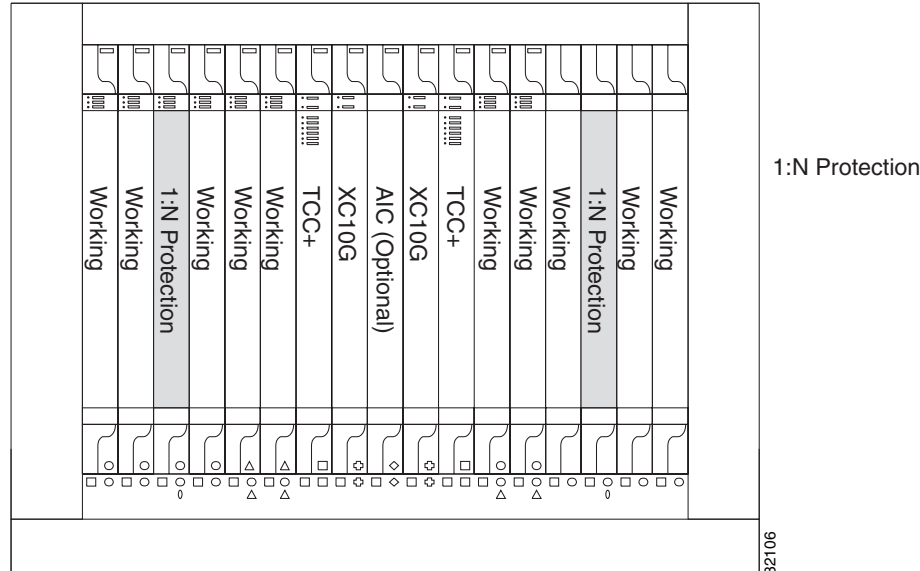
4.2.2.1 Revertive Switching

1:N protection supports revertive switching. Revertive switching sends the electrical interfaces (traffic) 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 the ONS 15454 software, Cisco Transport Controller (CTC). To set the revertive delay, see the *Cisco ONS 15454 Installation and Operations Guide*. All cards in a protection group share the same reversion settings. 1:N protection groups default to automatic reversion.

4.2.2.2 Protection Guidelines, 1:N

Several rules apply to 1:N protection groups in the ONS 15454:

- 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 may sit on either or both sides of the protect card

The ONS 15454 supports 1:N equipment protection for all add-drop multiplexer configurations (ring, linear, and terminal), as specified by Telcordia GR-253-CORE.

The ONS 15454 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.

For detailed procedures on setting up DS-1 and DS-3 protection groups, see the protection information in the *Cisco ONS 15454 Installation and Operations Guide*.

4.3 Electrical Card Protection and the Backplane

Protection schemes for electrical cards differ slightly depending on the Electrical Interface Assembly (EIA) type used on the ONS 15454 backplane. The difference is due to the varying connector size. For example, because BNC connectors are larger, fewer DS3-12 cards can be supported when using a BNC connector.

Note   For EIA descriptions and installation, see the *Cisco ONS 15454 Installation and Operations Guide*.

Caution   When a protection switch moves traffic from the DS3-12 working/active card to the DS3-12 protect/standby card, ports on the new active/standby card cannot be taken out of service as long as traffic is switched. Lost traffic can result when a port is taken out of service even if the DS3-12 standby card no longer carries traffic.

4.3.1 Standard BNC Protection

When you use BNC connectors, the ONS 15454 supports 1:1 protection or 1:N protection for a total of four working DS-3 electrical cards. If you are using EC-1 electrical cards with the BNC EIA, the ONS 15454 supports 1:1 protection and a total of four working cards. Slots 2, 4, 14 and 16 are designated working slots. These slots are mapped to a set of 12 BNC connectors on the EIA. These slots can be used without protection for unprotected DS-3 access.

With 1:N or 1:1 protection, Slots 1, 3, 15 and 17 are designated for protection when BNC connectors are used. With 1:N protection, Slots 3 and 15 are also designated for protection when BNC connectors are used. Slots 5, 6, 12, and 13 do not support DS3-12 cards when you use the regular BNC EIA.

4.3.2 High-Density BNC Protection

When you use the High-Density BNC EIA, the ONS 15454 supports 1:1 protection or 1:N protection for eight total working DS-3 electrical cards. If you are using EC-1 electrical cards with the High-Density BNC EIA, the ONS 15454 supports 1:1 protection and a total of eight working cards. Slots 1, 2, 4, 5, 13, 14, 16, and 17 are designated working slots.

These slots are mapped to a set of 12 BNC type connectors on the EIA. You can use these slots without protection for unprotected DS-3 or EC-1 access. Slots 3 and 15 are designated for 1:N protection slots when you use BNC connectors with the High-Density BNC EIA. Slots 6 and 12 do not support DS-3 or EC-1 cards when you use the High-Density BNC EIA.

4.3.3 SMB Protection

When you use SMB connectors, the ONS 15454 supports 1:1 or 1:N protection for the DS-1 and the DS-3 electrical cards. If you are using EC-1 cards with the SMB EIA, the ONS 15454 supports 1:1 protection. Working and protection electrical cards are defined by card slot pairs (the same card type is used for working and protect modules; the protection of the card is defined by the slot where it is housed). Each slot maps to a set of 12 or 14 SMB connectors on the EIA depending on the number of ports on the corresponding card. Any slot can be used without protection for unprotected DS-1, DS-3, or EC-1 access.

The DS1N-14 card can be a working or protect card in 1:1 or 1:N protection schemes. When used with 1:N protection, the DS1N-14 card can protect up to five DS1-14 plug-ins using the SMB connectors with the DS-1 electrical interface adapters (baluns).

4.3.4 AMP Champ Protection

When you use AMP Champ connectors, the ONS 15454 supports 1:1 or 1:N protection for the DS-1 cards. The DS1N-14 card can be a working or protect card in 1:1 or 1:N protection schemes. When used with 1:N protection, the DS1N-14 card can protect up to five DS1-14 plug-ins using the AMP Champ EIA.

4.4 Optical Card Protection

With 1+1 port-to-port protection, any number of ports on the protect card can be assigned to protect the corresponding ports on the working card. The working and protect cards do not have to be placed side by side in the node. A working card must be paired with a protect card of the same type, for example, an OC-3 card should be paired with another OC-3 card. The protection takes place on the port level, any number of ports on the protect card can be assigned to protect the corresponding ports on the working card.

For example, on a four-port card, you can assign one port as a protection port on the protect card (protecting the corresponding port on the working card) and leave three ports unprotected. Conversely, you can assign three ports as protection ports and leave one port unprotected.

Note   Currently, the OC-3 card is the only multiple port optical card. You cannot make protection groups on the same multiport 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.

1+1 span protection can be either revertive or non-revertive. 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.

You create and modify protection schemes using CTC software. For more information, see the *Cisco ONS 15454 Installation and Operations Guide*.

4.5 Unprotected Cards

Unprotected cards are not included in a protection scheme; therefore, a card failure or a signal error results in lost data. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15454 bandwidth. Figure 4-3 shows the ONS 15454 in an unprotected configuration. All cards are in a working state.

Figure 4-3   ONS 15454 in an unprotected configuration
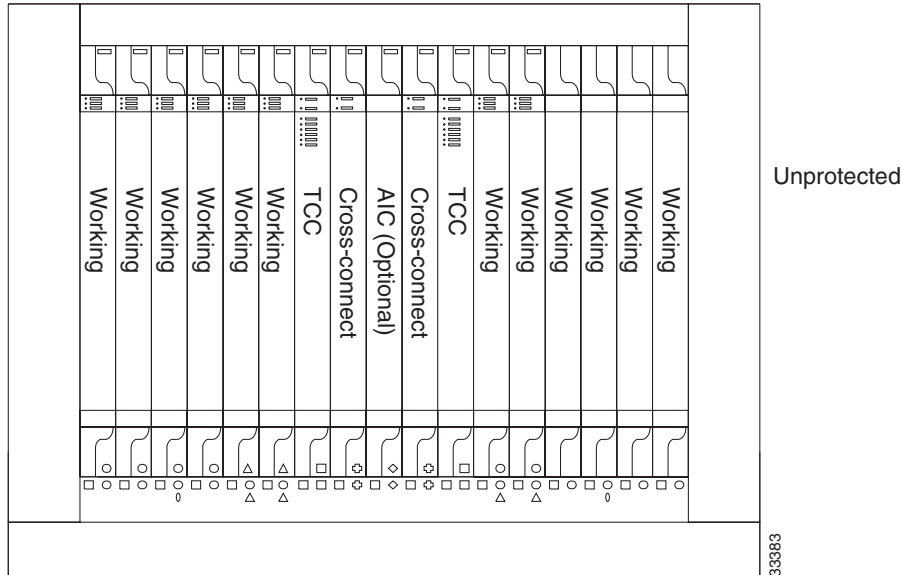
4.6 **Timing Communication and Control (TCC+) Card**
==

The TCC+ performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET Data Communications Channel (DCC) termination, and system fault detection for the ONS 15454. The TCC+ also ensures that the system maintains Telcordia timing requirements. Figure 4-4 shows the TCC+ faceplate and a block diagram of the card.

Figure 4-4   TCC+ faceplate and block diagram
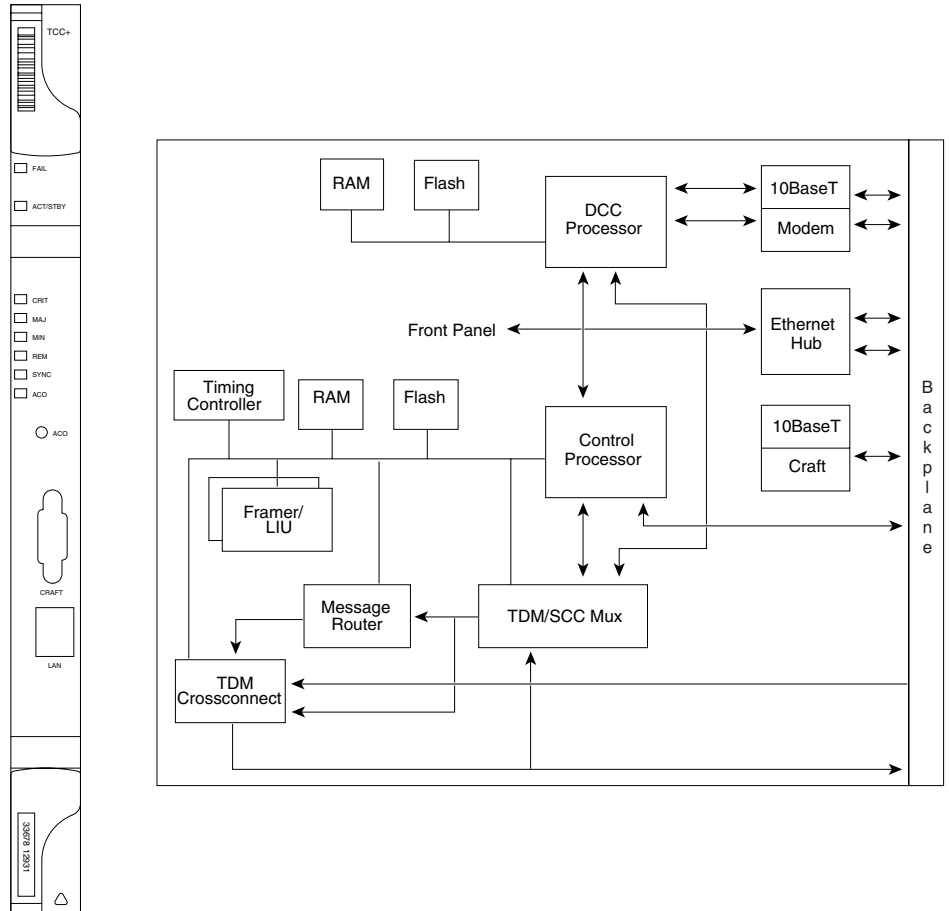
The node database, IP address, and system software are stored in TCC+ non-volatile memory, which allows quick recovery in the event of a power or card failure.

The TCC+ supports multichannel, high-level data link control (HDLC) processing for the DCC. Up to 48 DCCs can be routed over the Serial Communication Interface (SCI) and terminated at the TCC+. The TCC+ selects and processes ten DCCs to facilitate remote system management interfaces.

The TCC+ performs all system-timing functions for each ONS 15454. The TCC+ monitors the recovered clocks from each traffic card and two DS-1 (BITS) interfaces for frequency accuracy. The TCC+ selects a recovered clock, a BITS, or an internal Stratum 3 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+ to synchronize with the recovered clock, which provides holdover if the reference is lost.

Install TCC+ cards in Slots 7 and 11 for redundancy. If the active TCC+ fails, traffic switches to the protect TCC+. All TCC+ protection switches conform to protection switching standards of less than 50 ms.

The TCC+ features an RJ-45 10Base-T LAN port and an RS-232 DB9 type craft interface for user interfaces. The TL1 craft port runs at 9600 bps.

⚠

Caution   Cisco does not recommend operating the ONS 15454 with only one TCC+ card. To safeguard your
system, always operate in a redundant configuration.

4.6.1 TCC+ Card-Level Indicators

The TCC+ faceplate has eight LEDs. The first two LEDs are card-level indicators.

Table 4-14   TCC+ Card-Level Indicators

Card-Level LEDs	Definition
Red FAIL LED	Indicates a TCC+ hardware problem. Replace the unit if the FAIL LED persists.
ACT/STBY LED Green (Active) Amber (Standby)	The ACT/STBY (Active/Standby) LED indicates that the TCC+ is active (green) or in standby (amber). The ACT/STBY LED also provides the timing reference and shelf control. When the TCC+ is writing to the Active or Standby TCC+, its Active or Standby LED will blink. To avoid memory corruption, only remove the TCC+ when it is in standby and when the LED is not blinking.

4.6.2 Network-Level Indicators

The TCC+ faceplate has eight LEDs. Six LEDs are network-level indicators.

.

Table 4-15   TCC+ System-Level Indicators

System-Level LEDs	Definition
Red CRIT LED	Indicates a critical alarm in the network at the local node
Red MAJ LED	Indicates a major alarm in the network at the local node
Amber MIN LED	Indicates a minor alarm in the network at the local node
Red REM LED	Provides first-level alarm isolation. The REM LED turns red when an alarm is present in one or several of the remote nodes.
Green SYNC LED	Indicates 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. The ACO state is stopped if a new alarm occurs. After the originating alarm is cleared, the ACO LED and audible alarm control are reset.

4.6.3 TCC+ Specifications

- CTC Software
  - Interface: 10 Base-T LAN
  - Backplane access: wire wrap
- TL1 Craft Interface

- – Speed: 9600 baud

- – Front panel access: RS-232 DB9 type connector

- Synchronization

    - – Stratum 3, per Telcordia GR-253-CORE

    - – Free running access: accuracy 4.6 ppm

    - – Holdover Stability: 3.7 x10^{-7} ppm/day including temperature (<255 slips in first 24 hours)

    - – Reference: External BITS, line, internal

- Environmental

    - – Operating Temperature:

        C-Temp (15454-TCC+): 0 to +55 degrees Celsius

        I-Temp (15454-TCC+T): -40 to +65 degrees Celsius

    - – Operating Humidity: 5 - 95%, non-condensing

    - – Power Consumption: 9.82 W, 0.20 amps, 33.53 BTU/Hr.

- Dimensions

    - – Height: 12.650 in., Width: 0.716 in., Depth: 9.000 in.

    - – Card Weight: 1.5 lbs, 0.7 kg

- Compliance

    - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.7 XC Cross-Connect Card

The cross-connect card is the central element for ONS 15454 switching. Available cross-connects are the XC, XCVT, and XC10G. The XC establishes connections and performs time division switching (TDS) at the STS-1 level between ONS 15454 traffic cards. The XC card faceplate and block diagram are shown in Figure 4-5. The cross-connect matrix is shown in Figure 4-6 on page 4-20.

Figure 4-5   XC card faceplate and block diagram
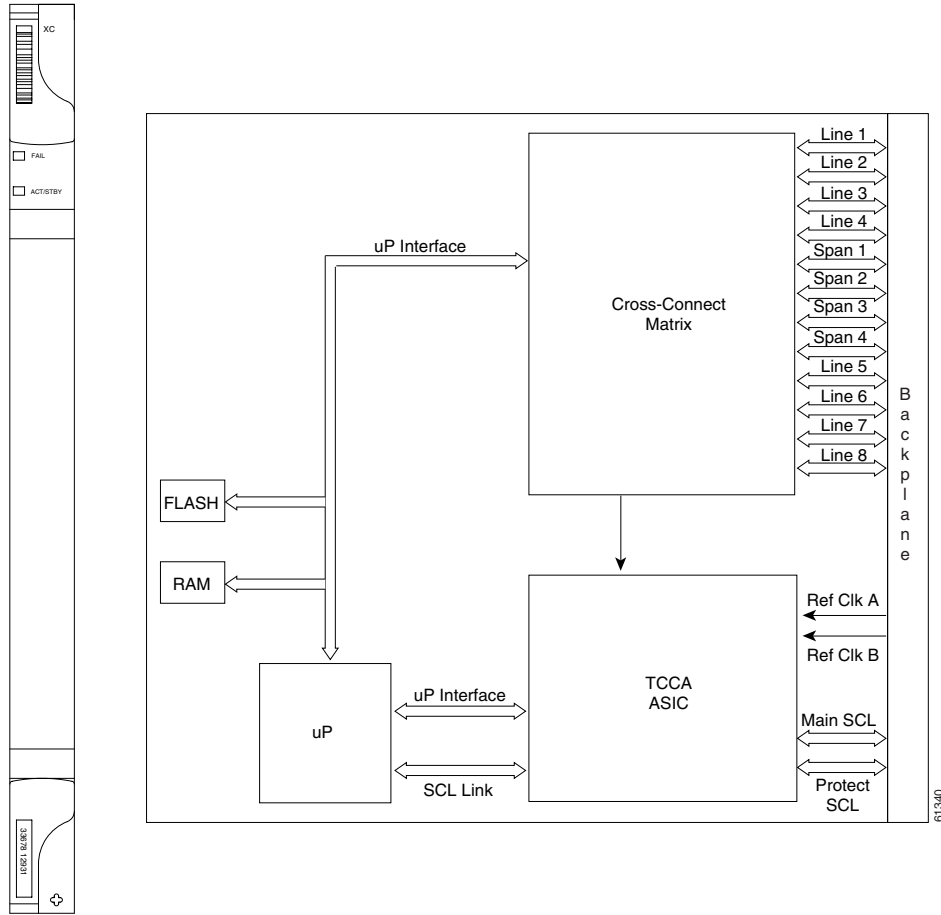
The switch matrix on the XC card consists of 288 bidirectional ports. When creating bidirectional STS-1 cross-connects, each cross-connect uses two STS-1 ports. This results in 144 bidirectional STS-1 cross-connects. The switch matrix is fully crosspoint, non-blocking, and broadcast supporting. (Any STS-1 on any port can be connected to any other port, meaning that the STS cross-connections are non blocking.) This allows network operators to concentrate or groom low-speed traffic from line cards onto high-speed transport spans and to drop low-speed traffic from transport spans onto line cards.

Figure 4-6   XC cross-connect matrix
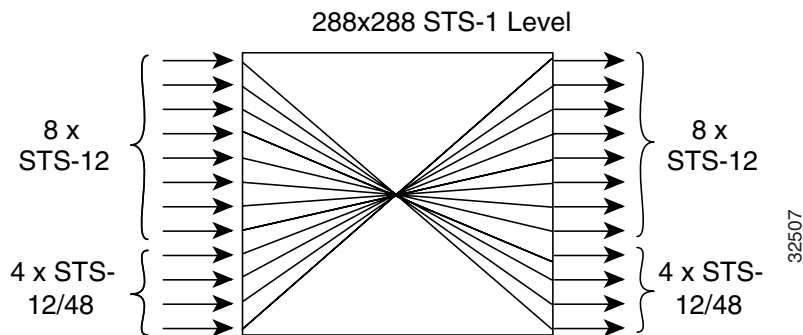
The XC card has 12 input ports and 12 output ports. Four input and output ports operate at either STS-12 or STS-48 rates. The remaining eight input and output ports operate at the STS-12 rate. An STS-1 on any of the input ports can be mapped to an STS-1 output port, thus providing full STS-1 time slot assignments (TSA).

The XC card works with the TCC+ card to maintain connections and set up cross-connects within the ONS 15454. Either the XC, XCVT, or XC10G is required to operate the ONS 15454. You establish cross-connect and provisioning information through CTC. The TCC+ establishes the proper internal cross-connect information and relays the setup information to the cross-connect card.

⚠

Caution   Do not operate the ONS 15454 with a single TCC+ card or a single XC/XCVT/XC10G card installed. Always operate the shelf with one working and one protect card of each type.

For simplex operation, you can install a single XC card in Slots 8 or 10. A second XC should be added for redundancy. The card has no external interfaces. All cross-connect card interfaces are provided through the ONS 15454 backplane.

4.7.1 XC Card-Level Indicators

The XC card faceplate has two card-level LEDs.

Table 4-16   XC Card-Level Indicators

Card-Level Indicators	Definition
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. If the FAIL LED persists, replace the card.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	The ACT/STBY LED indicates whether the XC card is active and carrying traffic (green) or in standby mode as a protect card (amber).

4.7.2 XC Specifications

- Cross-Connect
  - Connection Setup Time: 5 ms
  - Latency: 270 ns
- Environmental
  - Operating Temperature:

    C-Temp (15454-XC): 0 to +55 degrees Celsius

    I-Temp (15454-XC-T): -40 to +65 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 13 W, 0.28 amps, 46 BTU/Hr.
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.

- Depth: 9.000 in.
- Card Weight: 1.5 lbs, 0.7 kg
- Compliance
  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.8 XCVT Cross-Connect Card

The XCVT card provides the same STS capability as a standard XC card and also provides VT cross-connection. The XCVT provides non-blocking STS-48 capacity to all of the high-speed slots and non-bidirectional blocking STS-12 capacity to all multispeed slots. Any STS-1 on any port can be connected to any other port, meaning that the STS cross-connections are non blocking.

Figure 4-7 shows the XCVT faceplate and block diagram. Figure 4-8 on page 4-23 shows the cross-connect matrix.

Figure 4-7   XCVT faceplate and block diagram
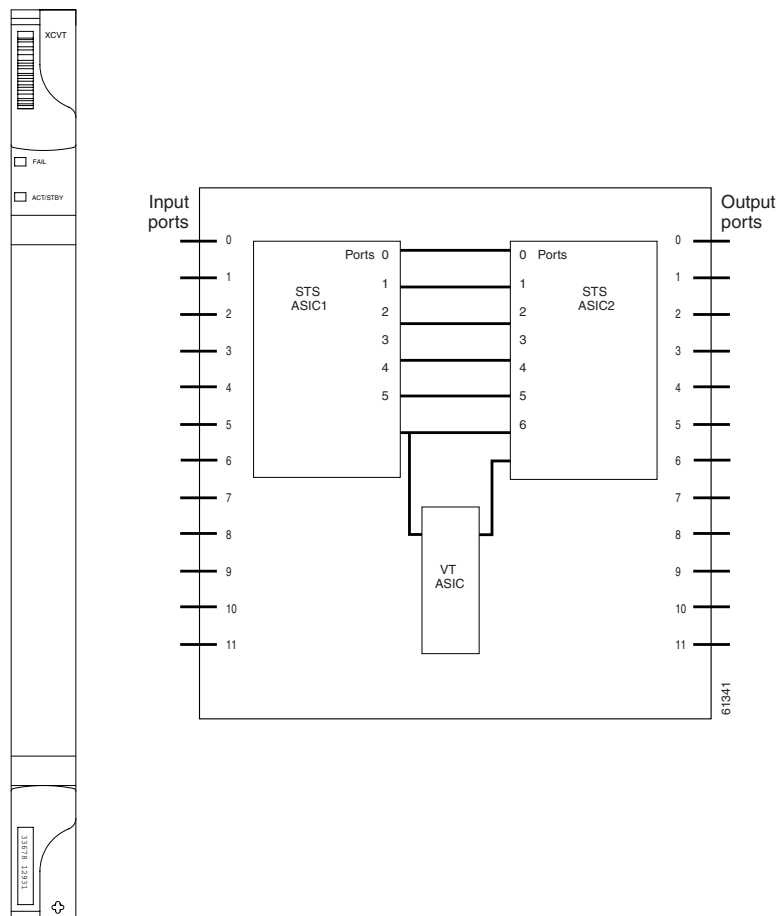
The STS-1 switch matrix on the XCVT card consists of 288 bidirectional ports and adds a VT matrix that can manage up to 336 bidirectional VT1.5 ports or the equivalent of a bidirectional STS-12. The VT1.5-level signals can be cross connected, dropped, or rearranged. The TCC+ assigns bandwidth to each slot on a per STS-1 or per VT1.5 basis. The switch matrices are fully crosspoint and broadcast supporting.

The XCVT card works with the TCC+ card to maintain connections and set up cross-connects within the node. Either the XCVT, XC10G, or XC is required to operate the ONS 15454. You can establish cross-connect (circuit) information through CTC. The TCC+ establishes the proper internal cross-connect information and relays the setup information to the XCVT card.

⚠

Caution   Do not operate the ONS 15454 with a single TCC+ card or a single XCVT/XC10G/XC card installed. Always operate the shelf with one working card and one protect card. Duplex cards must be the same type.

Figure 4-8   XCVT cross-connect matrix

Table 4-17   ONS 15454 VT Mapping
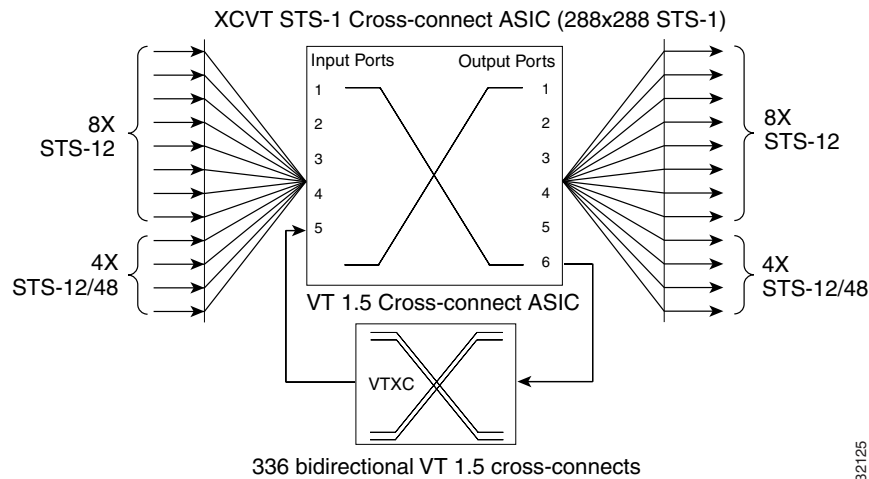
4.8.1 VT Mapping

The VT structure is designed to transport and switch payloads below the DS-3 rate. The Cisco ONS 15454 performs Virtual Tributary (VT) mapping according to Telcordia GR-253 standards. Table 4-17 shows the VT numbering scheme for the ONS 15454 as it relates to the Telcordia standard.

Table 4-17   ONS 15454 VT Mapping

ONS 15454 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1
VT5	Group5/VT1

Table 4-17   ONS 15454 VT Mapping (continued)

ONS 15454 VT Number	Telcordia Group/VT Number
VT6	Group6/VT1
VT7	Group7/VT1
VT8	Group1/VT2
VT9	Group2/VT2
VT10	Group3/VT2
VT11	Group4/VT2
VT12	Group5/VT2
VT13	Group6/VT2
VT14	Group7/VT2
VT15	Group1/VT3
VT16	Group2/VT3
VT17	Group3/VT3
VT18	Group4/VT3
VT19	Group5/VT3
VT20	Group6/VT3
VT21	Group7/VT3
VT22	Group1/VT4
VT23	Group2/VT4
VT24	Group3/VT4
VT25	Group4/VT4
VT26	Group5/VT4
VT27	Group6/VT4
VT28	Group7/VT4

4.8.2 XCVT Hosting DS3XM-6

The XCVT card works with DS3XM-6 (transmux) cards. A single DS3XM-6 can demultiplex (map down to a lower rate) six DS-3 signals into 168 VT1.5s that the XCVT card manages and cross connects. XCVT cards host a maximum of 336 bidirectional VT1.5s. In most network configurations, two DS3XM-6 cards are paired as working and protect cards.

4.8.3 XCVT Card-Level Indicators

The XCVT faceplate has two card-level LEDs.

Table 4-18   XCVT Card-Level Indicators

Card-Level Indicators	Definition
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	The ACT/STBY (Active/Standby) LED indicates whether the XCVT is active and carrying traffic (green) or in standby mode to the active XCVT card (amber).

4.8.4 XC/XCVT Compatibility

The XCVT card is compatible with the XC cards. The XCVT supports run-time compatibility with the XC cross-connect both within a single node and within a ring of mixed XCVT and XC nodes. However, working and protect cards within a single ONS 15454 must be either two XC cards or two XCVT cards. If an XC card or an XCVT card are used together as a working and protect pair, the XCVT acts as an XC card.

The XC and XCVT are supported in unidirectional path switched ring (UPSR) and bidirectional line switched ring (BLSR) configurations. VT and STS-level cross-connect and protection management are also supported in either type of ring. Nodes that rearrange or drop VTs must use an XCVT. Nodes that only rearrange or drop STSs can use an XC. You do not need to upgrade STS-only nodes to XCVT in a ring that can handle both VT and STS drop/rearrangement. In this scenario, however, the XC must run Software R2.0 or higher.

When upgrading from XC to XCVT cards, the first XCVT card installed acts as an XC card until the second XCVT card is installed. For more information, see Chapter 3, "Maintenance."

To create an STS-capable ring that allows VT drops at some nodes, all of the nodes in the ring must first run Software R2.0 or higher. The nodes that allow VT drops must use XCVT, but the nodes that do not allow VT drops can use the XC or XCVT card.

# 4.8.5 XCVT Card Specifications

- Environmental
  - Operating Temperature:

    C-Temp (15454-XC-VT): 0 to +55 degrees Celsius

    I-Temp (15454-XC-VT-T): -40 to +65 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 34.40 W, 0.72 amps, 117.46 BTU/Hr.
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.
  - Card Weight: 1.9 lbs, 0.8 kg
- Compliance

– ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.9 XC10G Cross-Connect Card

New to Software R3.1 is the XC10G card (Figure 4-9), which cross-connects STS-12, STS-48, and STS-192 signal rates. The XC10G allows up to four times the bandwidth of current XC and XCVT cards. The XC10G provides a maximum of 1152 STS-1 cross-connections. Any STS-1 on any port can be connected to any other port, meaning that the STS cross-connections are non blocking.

Figure 4-9 shows the XC10G faceplate and block diagram. shows the cross-connect matrix.

Figure 4-9   XC10G faceplate and block diagram
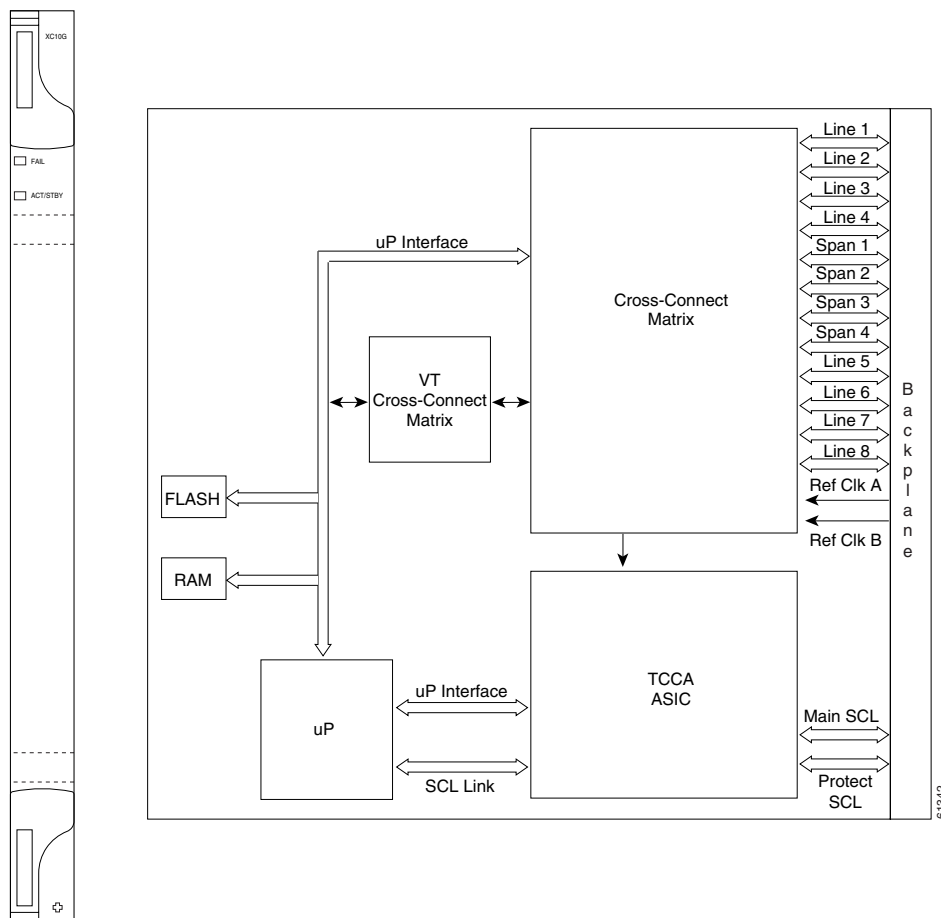
The XC10G card manages up to 336 bidirectional VT1.5 ports and 576 bidirectional STS-1 ports. The TCC+ assigns bandwidth to each slot on a per STS-1 or per VT1.5 basis.

Either the XC10G, XCVT, or XC is required to operate the ONS 15454. You can establish cross-connect (circuit) information through the Cisco Transport Controller (CTC). The TCC+ establishes the proper internal cross-connect information and sends the setup information to the cross-connect card.

⚠

Caution   Do not operate the ONS 15454 with a single TCC+ card or a single XC10G/XCVT/XC card installed. Always operate the shelf with one working and one protect card. Duplex cards must be the same type.

Figure 4-10   XC10G cross-connect matrix

XC10G STS-1 Cross-connect ASIC (1152x1152 STS-1)

Input Ports   Output Ports

1   1
2   2
.   .
.   .
.   .
.   .
25   25

8X STS-48
4X STS-192

8X STS-48
4X STS-192

VT 1.5 Cross-connect ASIC

VTXC

336 bidirectional VT 1.5 cross-connects

VT cross-connection occurs on the 25th port.

55386
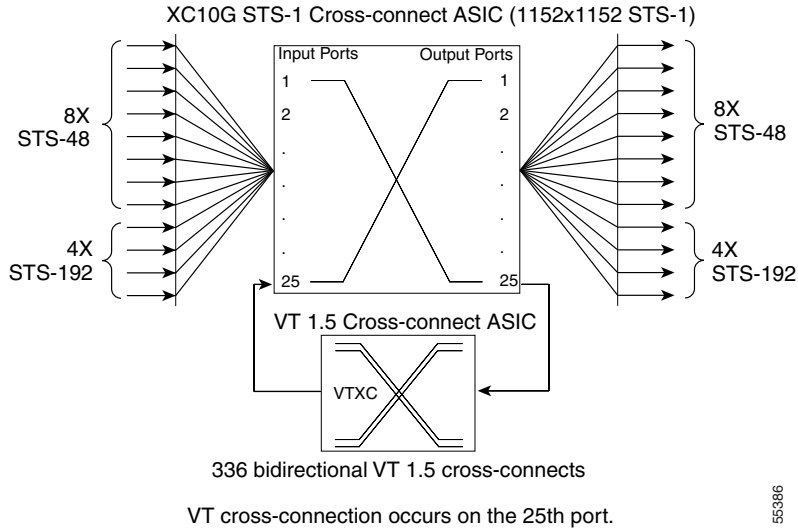
4.9.1 VT Mapping

The VT structure is designed to transport and switch payloads below the DS-3 rate. The Cisco ONS 15454 performs Virtual Tributary (VT) mapping according to Telcordia GR-253 standards. Table 4-19 shows the VT numbering scheme for the ONS 15454 as it relates to the Telcordia standard.

Table 4-19   ONS 15454 VT Mapping

ONS 15454 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1
VT5	Group5/VT1
VT6	Group6/VT1
VT7	Group7/VT1
VT8	Group1/VT2
VT9	Group2/VT2
VT10	Group3/VT2
VT11	Group4/VT2
VT12	Group5/VT2

Table 4-19   ONS 15454 VT Mapping (continued)

ONS 15454 VT Number	Telcordia Group/VT Number
VT13	Group6/VT2
VT14	Group7/VT2
VT15	Group1/VT3
VT16	Group2/VT3
VT17	Group3/VT3
VT18	Group4/VT3
VT19	Group5/VT3
VT20	Group6/VT3
VT21	Group7/VT3
VT22	Group1/VT4
VT23	Group2/VT4
VT24	Group3/VT4
VT25	Group4/VT4
VT26	Group5/VT4
VT27	Group6/VT4
VT28	Group7/VT4

4.9.2 XC10G Hosting DS3XM-6

The XC10G card works with the DS3XM-6 (transmux) card. A single DS3XM-6 can demultiplex (map down to a lower rate) six DS-3 signals into 168 VT1.5s that the XC10G card manages and cross connects. XC10G cards host a maximum of 336 bidirectional VT1.5 ports. In most network configurations, two DS3XM-6 cards are paired as working and protect cards.

4.9.3 XC10G Card-Level Indicators

The XC10G faceplate has two card-level LEDs.

Table 4-20   XC10G Card-Level Indicators

Card-Level Indicators	Definition
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. This LED illuminates during reset. The FAIL LED flashes during the boot process. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (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 (amber).

4.9.4 XC/XCVT/XC10G Compatibility

The XC10G supports the same features as the XC and XCVT cross-connects. The XC10G card is required for OC-192 and OC-48 any-slot operation. Do not use the XCVT or XC cards if you are using the OC-192 card, or if you placed one of the OC-48 any slot cards in a multispeed slot.

Note A configuration mismatch alarm occurs when a XC or XCVT cross-connect card coexists with an OC-192 card placed in the high-speed slot, or with an OC-48 card placed in the multispeed slot.

The TCC+ card, Software R3.1 or higher and the new 15454-SA-ANSI shelf assembly are required for the operation of the XC10G. If you are using Ethernet cards, the E1000-2-G or the E100T-G must be used when the XC10G cross-connect card is in use. Do not pair an XC or XCVT with an XC10G. When upgrading from XC or XCVT to the XC10G card, see the *Cisco ONS 15454 Installation and Operations Guide* for more information.

4.9.5 XC10G Card Specifications

- Environmental
  - Operating Temperature:

    C-Temp (15454-XC-10G): 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 85%, non-condensing
  - Power Consumption: 54 W, 1.12 amps, 184.38 BTU/Hr.
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.
  - Card Weight: 1.5 lbs, 0.6 kg
- Compliance
  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.10 Alarm Interface Controller Card

The optional Alarm Interface Controller (AIC) card provides customer-defined alarm input/output (I/O) and supports local and express orderwire. Figure 4-11 shows the AIC faceplate and a block diagram of the card. Figure 4-12 on page 4-32 shows the RJ-11 cable.

Figure 4-11   AIC faceplate and block diagram

4.10.1 User-Defined Alarms

The AIC card provides input/output alarm contact closures. You can define up to four external alarms and four external controls. The physical connections are made using the backplane wire-wrap pins. The alarms are defined using CTC and TL1. For instructions, see the *Cisco ONS 15454 Installation and Operations Guide*.

Each alarm contact has a corresponding LED on the front panel of the AIC that indicates the status of the alarm. 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 four 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), a 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 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:

- 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.

4.10.2 Orderwire

Orderwire allows a craftsperson to plug a phoneset into an ONS 15454 and communicate with craftspeople working at other ONS 15454s or other facility equipment. The orderwire is a pulse code modulation (PCM) encoded voice channel that uses E1 or E2 bytes in section/line overhead.

The AIC allows simultaneous use of both local (section overhead signal) and express (line overhead channel) orderwire channels on a SONET ring or particular optics facility. Local orderwire also allows communication at 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 SONET facility. The ONS 15454 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 BLSR and UPSR.

⚠️
Caution   Do not configure orderwire loops. Orderwire loops cause feedback that disables the orderwire channel.

The ONS 15454 implementation of both local and express orderwire is broadcast in nature. The line acts as a party line. There is no signalling for private point-to-point connections. 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 facilities for each local and express orderwire are provisionable as orderwire paths.

The AIC supports a "call" button on the module front panel which, when pressed, causes all ONS 15454 AICs on the orderwire subnetwork to "ring." The ringer/buzzer resides on the AIC. There is also a "ring" LED that mimics the AIC ringer. It flashes when any "call" button is pressed on the orderwire subnetwork. The "call" button and ringer/LED allow a remote craftsperson to get the attention of craftspeople across the network.

The orderwire ports are standard RJ-11 receptacles. The pins on the orderwire ports correspond to the tip and ring orderwire assignments.

Table 4-21   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

When provisioning the orderwire subnetwork, make sure that an orderwire loop does not exist. Loops cause oscillation and an unusable orderwire channel.

Figure 4-12   RJ-11 cable
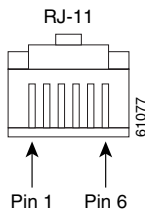
4.10.3 AIC Specifications

- Environmental
  - Operating Temperature:

    C-Temp (15454-AIC): 0 to +55 degrees Celsius

    I-Temp (15454-AIC-T): -40 to +65 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 6.01 W, 0.12 amps, 20.52 BTU/Hr.
- Dimensions
  - Height: 12.650 in., Width: 0.716 in., Depth: 9.000 in.
  - Card Weight: 1.6 lbs, 0.7 kg
- Compliance
  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.11 EC1-12 Card

The EC1-12 card provides 12 Telcordia-compliant, GR-253 STS-1 electrical ports per card. Each port operates at 51.840 Mbps over a single 75 ohm 728A or equivalent coaxial span. Figure 4-13 shows the EC1-12 faceplate and a block diagram of the card.

Figure 4-13   EC1-12 faceplate and block diagram
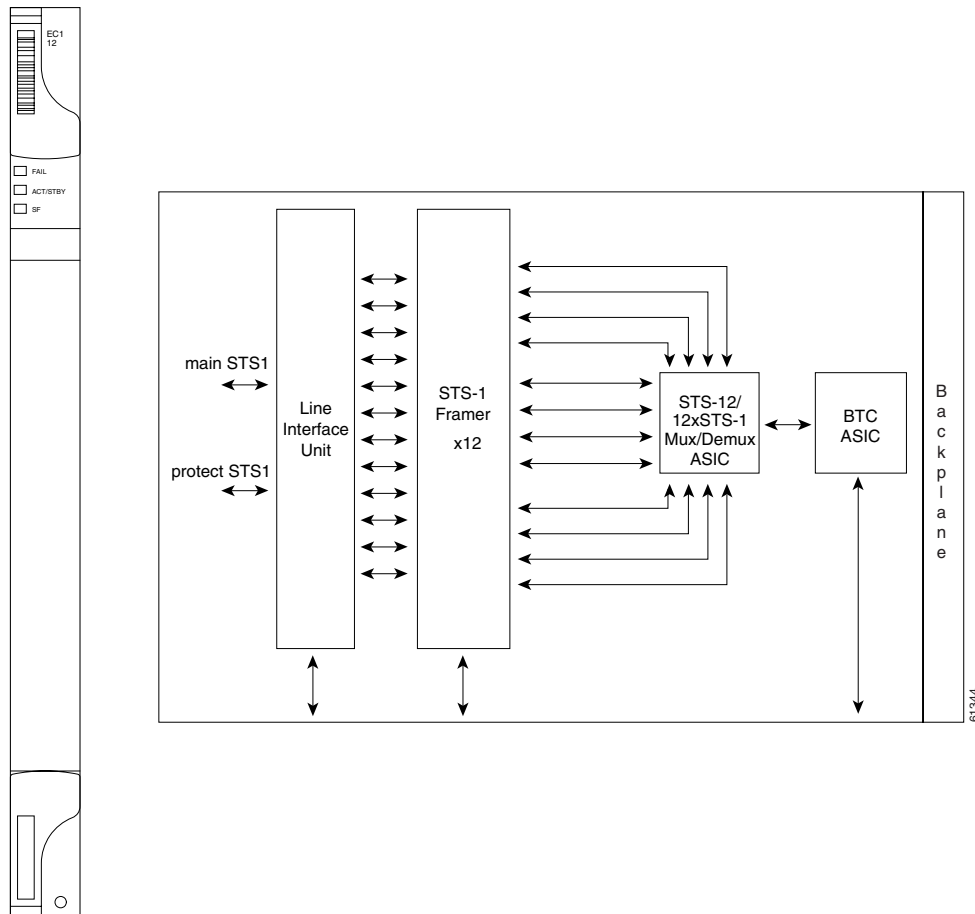
STS path selection for UNEQ-P, AIS-P, and bit error rate (BER) thresholds is done on the SONET ring interfaces (optical cards) in conjunction with the STS cross-connect. The EC1-12 terminates but does not select the 12 working STS-1 signals from the backplane. The EC1-12 maps each of the 12 received EC1 signals into 12 STS-1s with visibility into the SONET path overhead.

You can install the EC1-12 card in any multispeed or high-speed card slot on the ONS 15454. Each EC1-12 interface features DSX-level (digital signal cross-connect frame) outputs supporting distances up to 450 feet depending on facility conditions.

An EC1-12 card can be 1:1 protected with another EC1-12 card but cannot protect more than one EC1-12 card. You must install the EC1-12 in an even-numbered slot to serve as a working card and in an odd-numbered slot to serve as a protect card.

4.11.1 EC1-12 Hosted by XCVT

All 14 VT1.5 payloads from a EC1-12 card are carried in a single STS-1 to the XC or XCVT card where the payload is further aggregated for efficient STS-1 transport. XCVT cards host a maximum of 336 bidirectional VT1.5s.

4.11.2 EC1-12 Card-Level Indicators

The EC1-12 card faceplate has three card-level LEDs.

Table 4-22   EC1-12 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED signifies that the EC1-12 card's processor is not ready. Replace the unit if the FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the EC1-12 card is operational and ready to carry traffic.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as loss of signal (LOS), loss of frame (LOF) or high bit error rate (BER) on one or more of the card's ports.

4.11.3 EC1-12 Port-Level Indicators

You can obtain the status of the EC1-12 card ports using the LCD screen on the ONS 15454 fan-tray. 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.11.4 EC1-12 Specifications

- EC1-12 Input
  - Bit Rate: 51.84 Mbps +/- 20 ppm
  - Frame Format: SONET
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
  - AIS: TR-TSY-000191-compliant
- EC1-12 Output
  - Bit Rate: 51.84 Mbps +/- 20 ppm
  - Frame Format: SONET
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable

- – Input Impedance: 75 ohms +/-5%

- – Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179

- – AIS: TR-TSY-000191-compliant

- – Power Level: -1.8 - +5.7 dBm

- – Pulse Shape: ANSI T1.102-1988 Figure 8

- – Pulse Amplitude: 0.36 - 0.85 V peak to peak

- – Loopback Modes: Terminal and Facility

- – Line Build Out: 0-225 ft.; 226-450 ft.

- • EC1-12 Electrical Interface

  - – Connectors: BNC or SMB

- • Environmental

  - – Operating Temperature:

    C-Temp (15454-EC1-12): 0 to +55 degrees Celsius

    I-Temp (15454-EC1-12-T): -40 to +65 degrees Celsius

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 36.60 W, 0.76 amps, 124.97 BTU/Hr.

- • Dimensions

  - – Height: 12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 2.0 lbs, 0.9 kg

- • Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.12 DS1-14 Card

The ONS 15454 DS1-14 card provides 14 Telcordia-compliant, GR-499 DS-1 ports. Each port operates at 1.544 Mbps over a 100 ohm twisted-pair copper cable. The DS1-14 card can function as a working or protect card in 1:1 protection schemes and as a working card in 1:N protection schemes. Figure 4-14 shows the DS1-14 faceplate and a block diagram of the card.

Figure 4-14   DS1-14 faceplate and block diagram
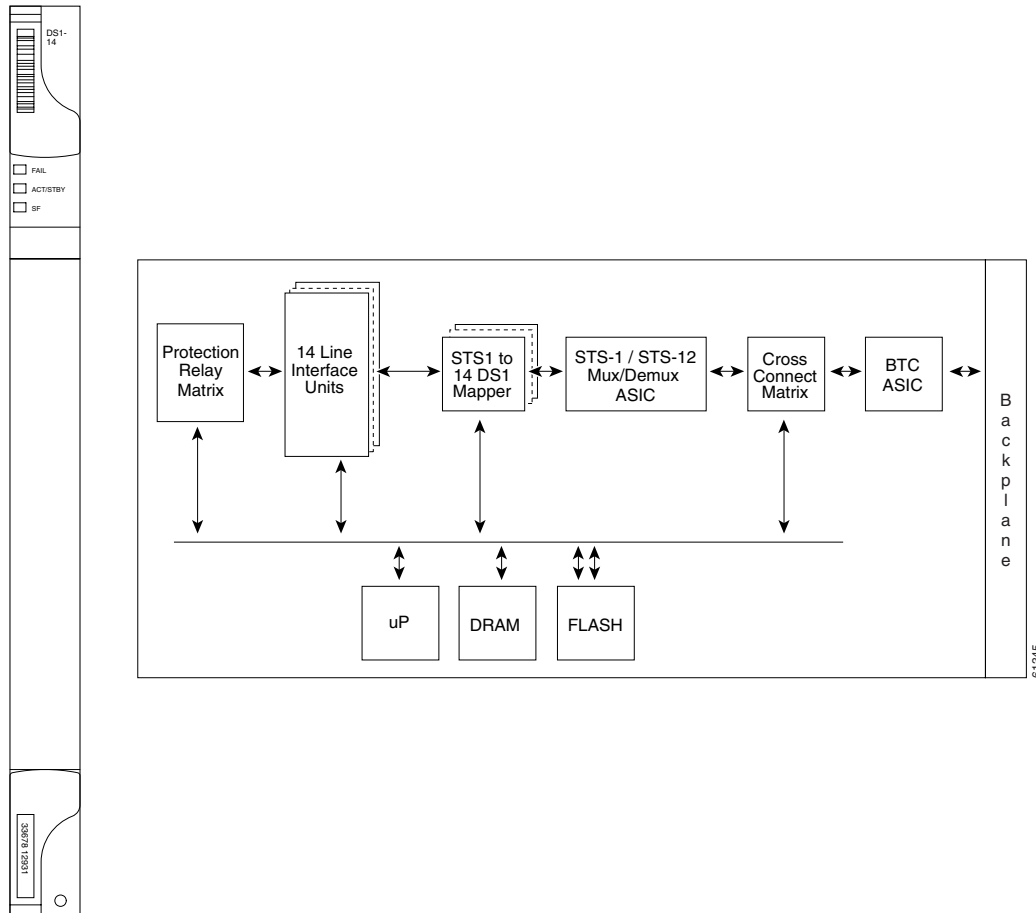
You can install the DS1-14 card in any multispeed or high-speed card slot on the ONS 15454. Each DS1-14 port has DSX-level (digital signal cross-connect frame) outputs supporting distances up to 655 feet.

The DS1-14 card supports 1:1 protection. The DS1-14 can be a working card in a 1:N protection scheme with the proper backplane EIA and wire-wrap or AMP Champ connectors. You can also provision the DS1-14 to monitor for line and frame errors in both directions.

You can group and map DS1-14 card traffic in STS-1 increments to any other card in an ONS 15454 except DS-3 cards. Each DS-1 is asynchronously mapped into a SONET VT1.5 payload and the card carries a DS-1 payload intact in a VT1.5. For performance monitoring purposes, you can gather bidirectional DS-1 frame-level information (loss of frame, parity errors, cyclic redundancy check [CRC] errors, etc.).

4.12.1 DS1-14 Hosted by XCVT

All 14 VT1.5 payloads from a DS1-14 card are carried in a single STS-1 to the XC or XCVT card where the payload is further aggregated for efficient STS-1 transport. XCVT cards host a maximum of 336 bidirectional VT1.5s.

4.12.2 DS1-14 Card-Level Indicators

The DS1-14 card faceplate has three LEDs.

Table 4-23   DS1-14 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	The green/amber ACT/STBY LED indicates whether the DS1-14 card is operational and ready to carry traffic (green) or in standby mode (amber).
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on one or more of the card's ports.

4.12.3 DS1-14 Port-Level Indicators

You can obtain the status of the DS1-14 card ports using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.12.4 DS1-14 Specifications

- DS1-14 Input
    - Bit Rate: 1.544 Mbps +/- 32 ppm
    - Frame Format: Off, SF (D4), ESF
    - Line Code: AMI, B8ZS
    - Termination: Wire-wrap, AMP Champ
    - Input Impedance:100 ohms
    - Cable Loss: Max 655 ft. ABAM #22 AWG
    - AIS: TR-TSY-000191-compliant
- DS1-14 Output
    - Bit Rate: 1.544 Mbps +/- 32 ppm
    - Frame Format: Off, SF (D4), ESF
    - Line Code: AMI, B8ZS
    - Termination: Wire-wrap, AMP Champ
    - Input Impedance:100 ohms
    - Cable Loss: Max 655 ft. ABAM #22 AWG
    - AIS: TR-TSY-000191-compliant
    - Power Level: 12.5 to 17.9 dBm centered @ 772 KHz, -16.4 to -11.1 dBm centered at 1544 KHz

- Pulse Shape: GR-499-CORE Figure 9-5

- Pulse Amplitude: 2.4- 3.6 V peak-to-peak

- Loopback Modes: Terminal and Facility

- Environmental

  - Surge Protection: GR-1089

  - Operating Temperature:

    C-Temp (15454-DS1-14): 0 to +55 degrees Celsius

    I-Temp (15454-DS1-14-T): -40 to +65 degrees Celsius

  - Operating Humidity: 5 - 95%, non-condensing

  - Power Consumption: 12.60 W, 0.26 amps, 43.02 BTU/Hr.

- Dimensions

  - Height: 12.650 in.

  - Width: 0.716 in.

  - Depth: 9.000 in.

  - Card Weight: 1.8 lbs, 0.8 kg

- Compliance

  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.13 DS1N-14 Card

The DS1N-14 card provides 14 Telcordia-compliant, GR-499 DS-1 ports. Each DS1N-14 port operates at 1.544 Mbps over a 100 ohm twisted-pair copper cable. Figure 4-15 shows the DS1N-14 faceplate and a block diagram of the card.

Figure 4-15   DS1N-14 faceplate and block diagram
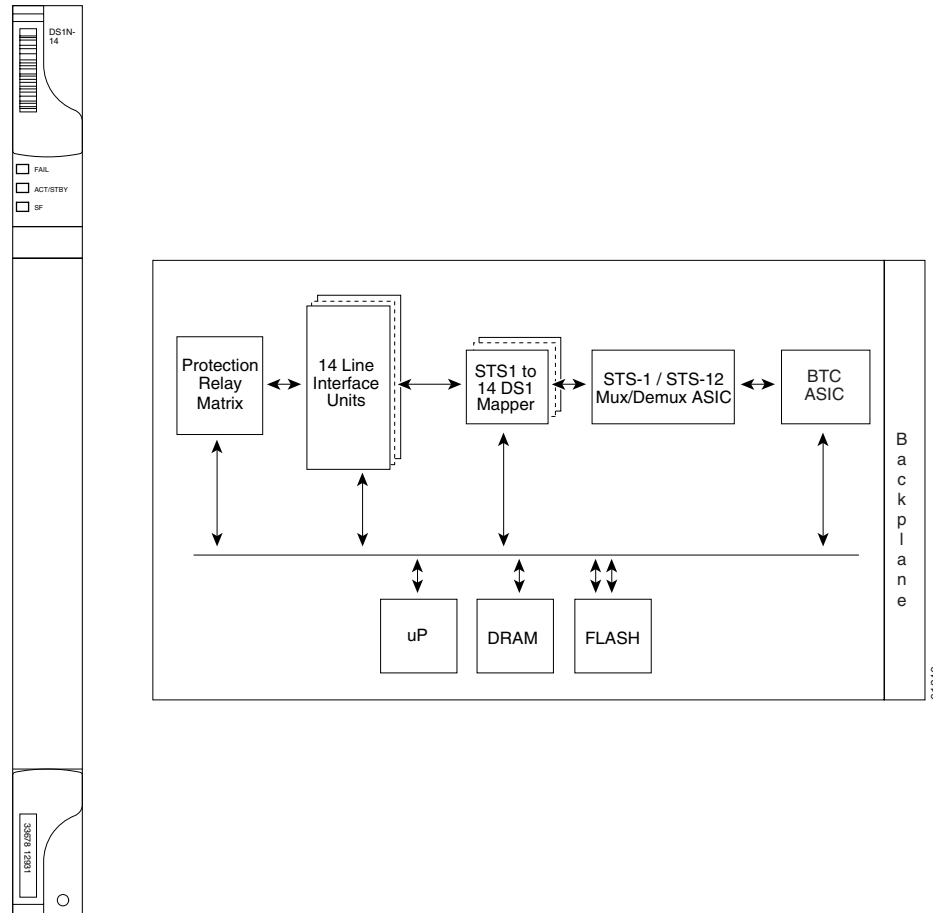
Each DS1N-14 port features DSX-level outputs supporting distances up to 655 feet depending on facility conditions.

The DS1N-14 card supports 1:N (N≤5) protection with the proper backplane EIA and wire-wrap or AMP Champ connectors. You can also provision the DS1N-14 to monitor line and frame errors in both directions.

The DS1N-14 card can function as a working or protect card in 1:1 or 1:N protection schemes. If you use the DS1N-14 as a standard DS-1 card in a 1:1 protection group, you can install the DS1N-14 card in any multispeed or high-speed card slot on the ONS 15454. If you use the card's 1:N functionality, you must install a DS1N-14 card in Slots 3 and 15.

You can group and map DS1N-14 card traffic in STS-1 increments to any other card in an ONS 15454 node. Each DS-1 is asynchronously mapped into a SONET VT1.5 payload and the card carries a DS-1 payload intact in a VT1.5. For performance-monitoring purposes, you can gather bidirectional DS-1 frame-level information (loss of frame, parity errors or CRC errors, for example).

4.13.1 DS1N-14 Hosted by XCVT

All 14 VT1.5 payloads from a DS1N-14 card are carried in a single STS-1 to the XC or XCVT card where the payload is further aggregated for efficient STS-1 transport. XCVT cards host a maximum of 336 bidirectional VT1.5s.

4.13.2 DS1N-14 Card-Level Indicators

The DS1N-14 card faceplate has three LEDs.

Table 4-24   DS1N-14 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	The ACT/STBY LED indicates when the DS1N-14 card is operational and ready to carry traffic (green) or when the card is in standby mode (amber).
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on one or more of the card's ports.

4.13.3 DS1N-14 Port-Level Indicators

You can obtain the status of the 14 DS-1 ports using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.13.4 DS1N-14 Specifications

- DS1N-14 Input
  - Bit Rate: 1.544 Mbps +/- 32 ppm
  - Frame Format: Off, SF (D4), ESF
  - Line Code: AMI, B8ZS
  - Termination: Wire-wrap, AMP Champ
  - Input Impedance:100 ohms
  - Cable Loss: Max 655 ft. ABAM #22 AWG
  - AIS: TR-TSY-000191-compliant
- DS1N-14 Output
  - Bit Rate: 1.544 Mbps +/- 32 ppm
  - Frame Format: Off, SF (D4), ESF
  - Line Code: AMI, B8ZS
  - Termination: Wire-wrap, AMP Champ
  - Input Impedance:100 ohms
  - Cable Loss: Max 655 ft. ABAM #22 AWG
  - AIS: TR-TSY-000191-compliant
  - Power Level: 12.5 to 17.9 dBm centered @ 772 KHz, -16.4 to -11.1 dBm centered at 1544 KHz

- – Pulse Shape: GR-499-CORE Figure 9-5

- – Pulse Amplitude: 2.4- 3.6 V peak-to-peak

- – Loopback Modes: Terminal and Facility

- Environmental

  - – Surge Protection: GR-1089

  - – Operating Temperature:

    C-Temp (15454-DS1N-14): 0 to +55 degrees Celsius

    I-Temp (15454-DS1N-14-T): -40 to +65 degrees Celsius

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 12.60 W, 0.26 amps, 43.02 BTU/Hr.

- Dimensions

  - – Height: 12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 1.9 lbs, 0.8 kg

- Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.14 DS3-12 Card

The ONS 15454 DS3-12 card provides 12 Telcordia-compliant, GR-499 DS-3 ports per card. Each port operates at 44.736 Mbps over a single 75 ohm 728A or equivalent coaxial span. The DS3-12 card operates as a working or protect card in 1:1 protection schemes and as a working card in 1:N protection schemes. Figure 4-16 shows the DS3-12 faceplates, and a block diagram of the card.

Figure 4-16   DS3-12 faceplate and block diagram
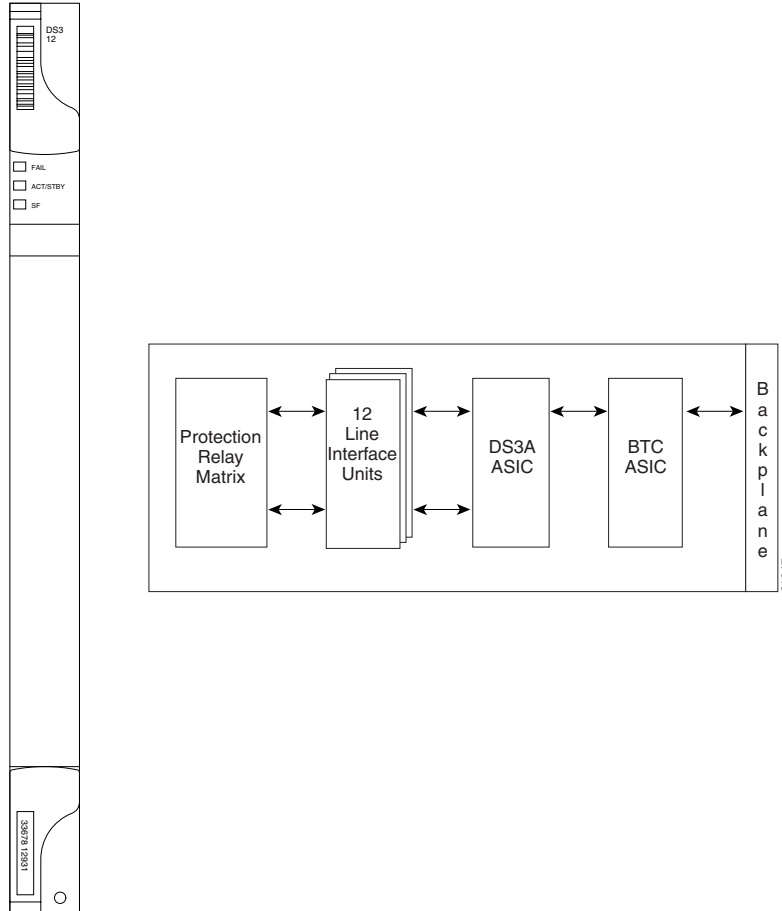
You can install the DS3-12 card in any multispeed or high-speed card slot on the ONS 15454. Each DS3-12 card port features DSX-level outputs supporting distances up to 450 feet depending on facility conditions.

The DS3-12 card supports 1:1 protection with the proper backplane EIA. EIAs are available with BNC or SMB connectors. For more information, see the "Electrical Card Protection and the Backplane" section on page 4-14.

⚠ **Caution**   When a protection switch moves traffic from the DS3-12 working/active card to the DS3-12 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 DS3-12 standby card no longer carries traffic.

4.14.1 DS3-12 Card-Level Indicators

The DS3-12 card faceplate has three LEDs.

Table 4-25   DS3-12 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	When the ACTV/STBY LED is green, the DS3-12 card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the DS3-12 card is operational and in standby (protect) mode.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as port LOS.

4.14.2 DS3-12 Port-Level Indicators

You can find the status of the 12 DS3-12 card ports using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.14.3 DS3-12 Specifications

- DS3-12 Input
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
  - AIS: TR-TSY-000191-compliant
- DS3-12 Output
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm
  - Pulse Shape: ANSI T1.102-1988 Figure 8
  - Pulse Amplitude: 0.36 - 0.85 V peak-to-peak
  - Loopback Modes: Terminal and Facility
- DS3-12 Electrical Interface

- – Connectors: BNC or SMB
- Environmental
  - – Operating Temperature:

    C-Temp (15454-DS3-12): 0 to +55 degrees Celsius

    I-Temp (15454-DS3-12-T): -40 to +65 degrees Celsius
  - – Operating Humidity: 5 - 95%, non-condensing
  - – Power Consumption: 38.20 W, 0.79 amps, 130.43 BTU/Hr.
- Dimensions
  - – Height: 12.650 in.
  - – Width: 0.716 in.
  - – Depth: 9.000 in.
  - – Card Weight: 1.7 lbs, 0.7 kg
- Compliance
  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.15 DS3N-12 Card

The ONS 15454 DS3N-12 card provides 12 Telcordia-compliant, TR499 DS-3 ports per card. Each port operates at 44.736 Mbps over a single 75 ohm 728A or equivalent coaxial span. Figure 4-17 shows the DS3N-12 faceplate and a diagram of the card.

Figure 4-17   DS3N-12 faceplate and block diagram
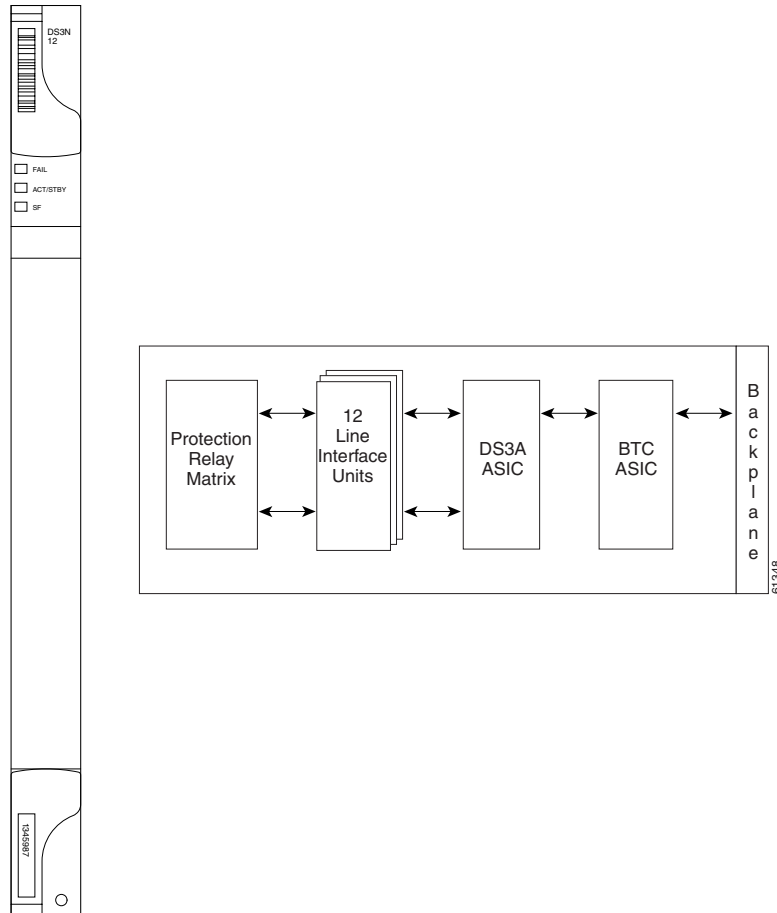
You can install the DS3N-12 card in any multispeed or high-speed card slot. Each DS3N-12 card port features DSX-level outputs supporting distances up to 450 feet depending on facility conditions. With the proper backplane EIA, the card supports BNC or SMB connectors.

The DS3N-12 can operate as the protect card in a 1:N (N≤5) DS-3 protection group. It has additional circuitry not present on the basic DS3-12 card that allows it to protect up to five working DS3-12 cards. The basic DS3-12 card can only function as the protect card for one other DS3-12 card. Other than the protection capabilities, the DS3-12 and DS3N-12 cards are identical.

4.15.1 DS3N-12 Card-Level Indicators

The DS3N-12 card faceplate has three LEDs.

Table 4-26   DS3N-12 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED Green (Active) Amber (Standby)	When the ACTV/STBY LED is green, the DS3N-12 card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the DS3N-12 card is operational and in standby (protect) mode.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as port LOS, AIS, etc.

4.15.2 DS3N-12 Port-Level Indicators

You can find the status of the 12 DS3N-12 card ports using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.15.3 DS3N-12 Card Specifications

- DS3N-12 Input
    - Bit Rate: 44.736 Mbps +/- 20 ppm
    - Frame Format: DS-3 ANSI T1.107-1988
    - Line Code: B3ZS
    - Termination: Unbalanced coaxial cable
    - Input Impedance: 75 ohms +/-5%
    - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
    - AIS: TR-TSY-000191-compliant
- DS3N-12 Output
    - Bit Rate: 44.736 Mbps +/- 20 ppm
    - Frame Format: DS-3 ANSI T1.107-1988
    - Line Code: B3ZS
    - Termination: Unbalanced coaxial cable
    - Input Impedance: 75 ohms +/-5%
    - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
    - AIS: TR-TSY-000191-compliant
    - Power Level: -1.8 - +5.7 dBm
    - Pulse Shape: ANSI T1.102-1988 Figure 8
    - Pulse Amplitude: 0.36 - 0.85 V peak-to-peak
    - Loopback Modes: Terminal and Facility

- Line Build Out: 0-225 ft.; 226-450 ft.
- DS3N-12 Electrical Interface
    - Connectors: BNC or SMB
- Environmental
    - Operating Temperature:

        C-Temp (15454-DS3N-12): 0 to +55 degrees Celsius

        I-Temp (15454-DS3N-12-T): -40 to +65 degrees Celsius
    - Operating Humidity: 5 - 95%, non-condensing
    - Power Consumption: 38.20 W, 0.79 amps, 130.43 BTU/Hr.
- Dimensions
    - Height: 12.650 in.
    - Width: 0.716 in.
    - Depth: 9.000 in.
    - Card Weight: 1.8 lbs, 0.8 kg
- Compliance
    - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.16 DS3-12E Card

The ONS 15454 DS3-12E card provides 12 Telcordia-compliant ports per card. Each port operates at 44.736 Mbps over a single 75 ohm 728A or equivalent coaxial span. The DS3-12E card provides enhanced performance monitoring functions. The DS3-12E can detect several different errored logic bits within a DS-3 frame. This function allows the ONS 15454 to identify a degrading DS-3 facility caused by upstream electronics (DS-3 Framer). In addition, DS3 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. Figure 4-18 shows the DS3-12E faceplate and a diagram of the card.

Figure 4-18   DS3-12E faceplate and block diagram
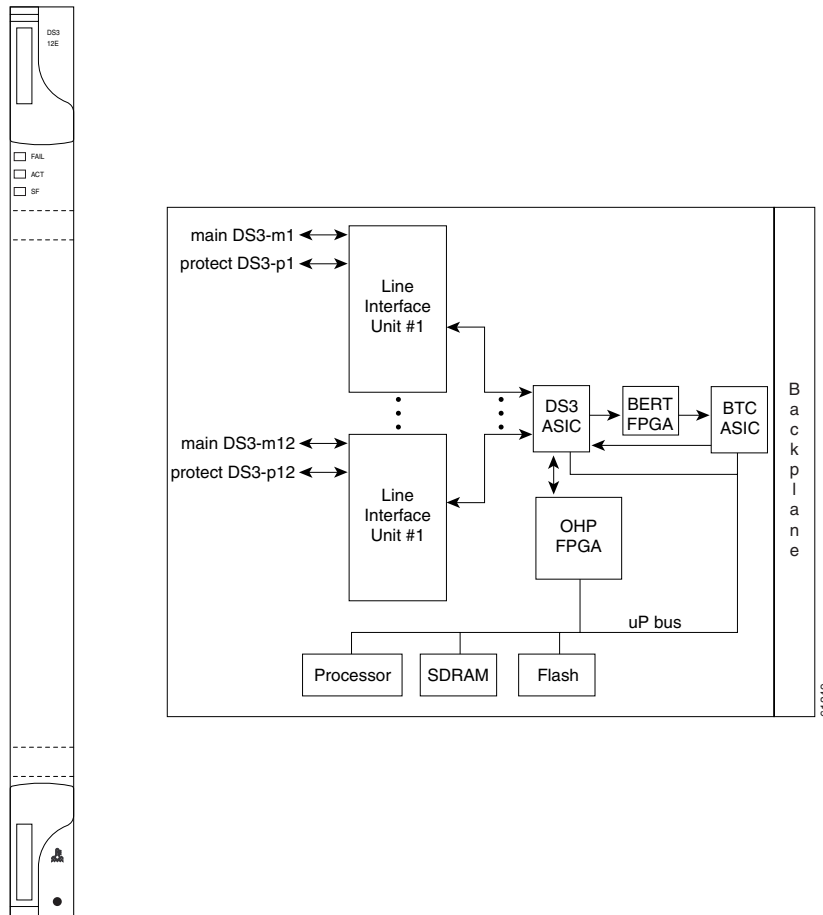
The following list summarizes DS3-12E card features:

- Provisionable framing format M23, C-bit or unframed
- Autorecognition and provisioning of incoming framing
- P-bit monitoring
- C-bit parity monitoring
- X-bit monitoring
- M-bit monitoring
- F-bit monitoring
- Far-end block errors (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 DS3-12E card in any multispeed or high-speed card slot on the ONS 15454. Each DS3-12E port features DSX-level outputs supporting distances up to 450 feet. With the proper backplane EIA, the card supports BNC or SMB connectors.

The DS3-12E supports a 1:1 protection scheme, meaning it can operate as the protect card for one other DS3-12E card.

4.16.1 DS3-12E Card-Level Indicators

The DS3-12E card faceplate has three LEDs.

Table 4-27   DS3-12E Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	When the ACTV/STBY LED is green, the DS3-12E card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the DS3-12E card is operational and in standby (protect) mode.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as port LOS, AIS, etc.

4.16.2 DS3-12E Port-Level Indicators

You can find the status of the DS3-12E card ports using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.16.3 DS3-12E Compatibility

The DS3-12E is compatible with Software R2.2.x or higher. If Software R3.0 or higher is used, the card uses all enhanced performance monitoring functions. With Software R2.2.2, the DS-3E card operates with the same functions as the older DS-3 card.

4.16.4 DS3-12E Card Specifications

- DS3-12E Input
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
  - AIS: TR-TSY-000191-compliant
- DS3-12E Output
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS

  - Termination: Unbalanced coaxial cable

  - Input Impedance: 75 ohms +/-5%

  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179

  - AIS: TR-TSY-000191-compliant

  - Power Level: -1.8 - +5.7 dBm (The power level is for a signal of all ones and is measured at a center frequency of 22.368 MHz (+/-KHz) bandwidth.)

  - Pulse Shape: ANSI T1.102-1988 Figure 8

  - Pulse Amplitude: 0.36 - 0.85 V peak-to-peak

  - Loopback Modes: Terminal and Facility

  - Line Build Out: 0-225 ft.; 226-450 ft.

- DS3-12E Electrical Interface

  - Connectors: BNC or SMB

- Environmental

  - Operating Temperature:

    I-Temp (15454-DS3-12E-T): -40 to +65 degrees Celsius

  - Operating Humidity: 5 - 95%, non-condensing

  - Power Consumption: 26.80 W, 0.56 amps, 91.51 BTU/Hr.

- Dimensions

  - Height: 12.650 in., Width: 0.716 in., Depth: 9.000 in.

  - Depth with backplane connector: 9.250 in.

  - Card Weight: 1.8 lbs, 0.8 kg

- Compliance

  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.17 DS3N-12E Card

The ONS 15454 DS3N-12E card provides 12 Telcordia-compliant ports per card. Each port operates at 44.736 Mbps over a single 75 ohm 728A or equivalent coaxial span. The DS3N-12E card provides enhanced performance monitoring functions. The DS3N-12E can detect several different errored logic bits within a DS-3 frame. This function allows the ONS 15454 to identify a degrading DS-3 facility caused by upstream electronics (DS-3 Framer). In addition, DS3 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. Figure 4-19 shows the DS3N-12E faceplate and a diagram of the card.

Figure 4-19   DS3N-12E faceplate and block diagram
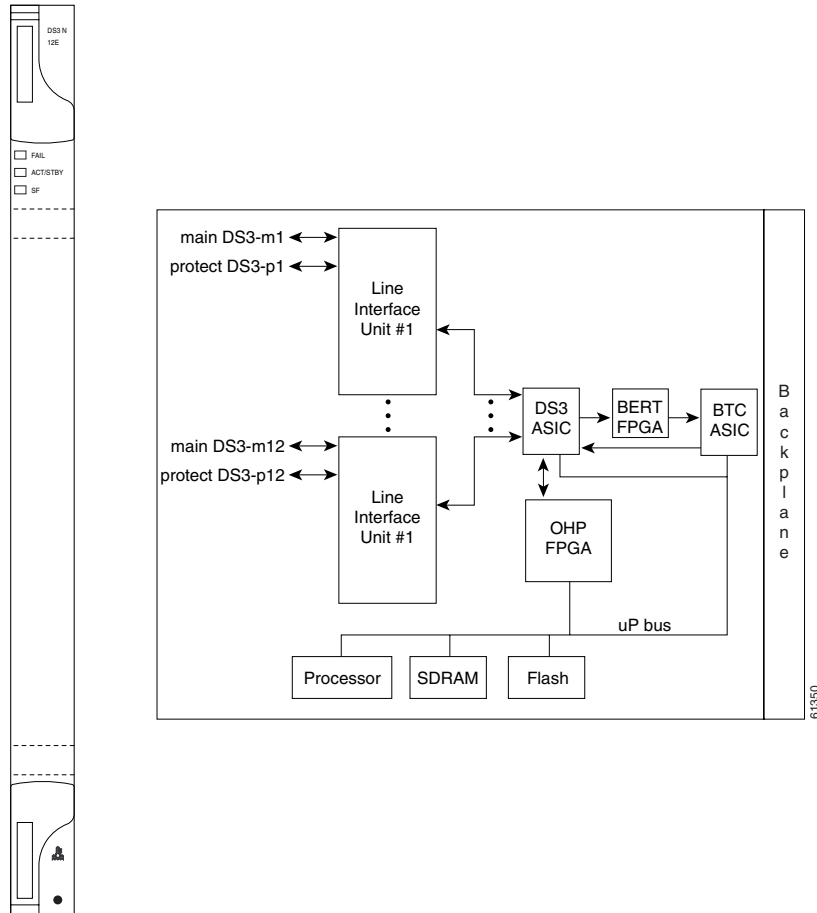
The following list summarizes the DS3N-12E card features:

- Provisionable framing format M23, C-bit or unframed
- Autorecognition and provisioning of incoming framing
- P-bit monitoring
- C-bit parity monitoring
- X-bit monitoring
- M-bit monitoring
- F-bit monitoring
- Far-end block errors (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 DS3N-12E card in any multispeed or high-speed card slot. Each DS3N-12E port features DSX-level outputs supporting distances up to 450 feet. With the proper backplane EIA, the card supports BNC or SMB connectors.

The DS3N-12E can operate as the protect card in a 1:N (N≤5) DS-3 protection group. It has additional circuitry not present on the basic DS3-12E card that allows it to protect up to five working DS3-12E cards. The basic DS3-12E card can only function as the protect card for one other DS3-12E card.

4.17.1 DS3N-12E Card-Level Indicators

The DS3N-12E card faceplate has three LEDs.

Table 4-28   DS3N-12E Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	When the ACTV/STBY LED is green, the DS3N-12E card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the DS3N-12E card is operational and in standby (protect) mode.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as AIS, LOS, or LOF on one or more of the card's ports.

4.17.2 DS3N-12E Port-Level Indicators

You can find the status of the DS3N-12E card ports using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.17.3 DS3N-12E Compatibility

The DS3N-12E cards are compatible with Software R2.2.x or higher. If Software R3.0 or higher is used, the DS3N-12E operates using all enhanced performance monitoring functions. With Software R2.2.2, the DS3N-12E operates with the same functions as the older DS-3 card.

4.17.4 DS3N-12E Card Specifications

- DS3N-12E Input
    - Bit Rate: 44.736 Mbps +/- 20 ppm
    - Frame Format: DS-3 ANSI T1.107-1988
    - Line Code: B3ZS
    - Termination: Unbalanced coaxial cable
    - Input Impedance: 75 ohms +/-5%
    - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
    - AIS: TR-TSY-000191-compliant
- DS3N-12E Output

- Bit Rate: 44.736 Mbps +/- 20 ppm

- Frame Format: DS-3 ANSI T1.107-1988

- Line Code: B3ZS

- Termination: Unbalanced coaxial cable

- Input Impedance: 75 ohms +/-5%

- Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179

- AIS: TR-TSY-000191-compliant

- Power Level: -1.8 - +5.7 dBm (The power level is for a signal of all ones and is measured at a center frequency of 22.368 MHz (+/-KHz) bandwidth.)

- Pulse Shape: ANSI T1.102-1988 Figure 8

- Pulse Amplitude: 0.36 - 0.85 V peak-to-peak

- Loopback Modes: Terminal and Facility

- Line Build Out: 0-225 ft.; 226-450 ft.

- DS3N-12E Electrical Interface

  - Connectors: BNC or SMB

- Environmental

  - Operating Temperature:

    I-Temp (15454-DS3N-12E-T): -40 to +65 degrees Celsius

  - Operating Humidity: 5 - 95%, non-condensing

  - Power Consumption: 26.80 W, 0.56 amps, 91.51 BTU/Hr.

- Dimensions

  - Height: 12.650 in., Width: 0.716 in., Depth: 9.000 in.

  - Depth with backplane connector: 9.250 in.

  - Card Weight: 1.9 lbs, 0.8 kg

- Compliance

  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.18 DS3XM-6 Card

The DS3XM-6 card, commonly referred to as a transmux card, provides six Telcordia-compliant, GR-499-CORE M13 multiplexing functions. The DS3XM-6 converts six framed DS-3 network connections to 28x6 or 168 VT1.5s. shows the DS3XM-6 faceplate and a block diagram of the card.

Figure 4-20   DS3XM-6 faceplate and block diagram
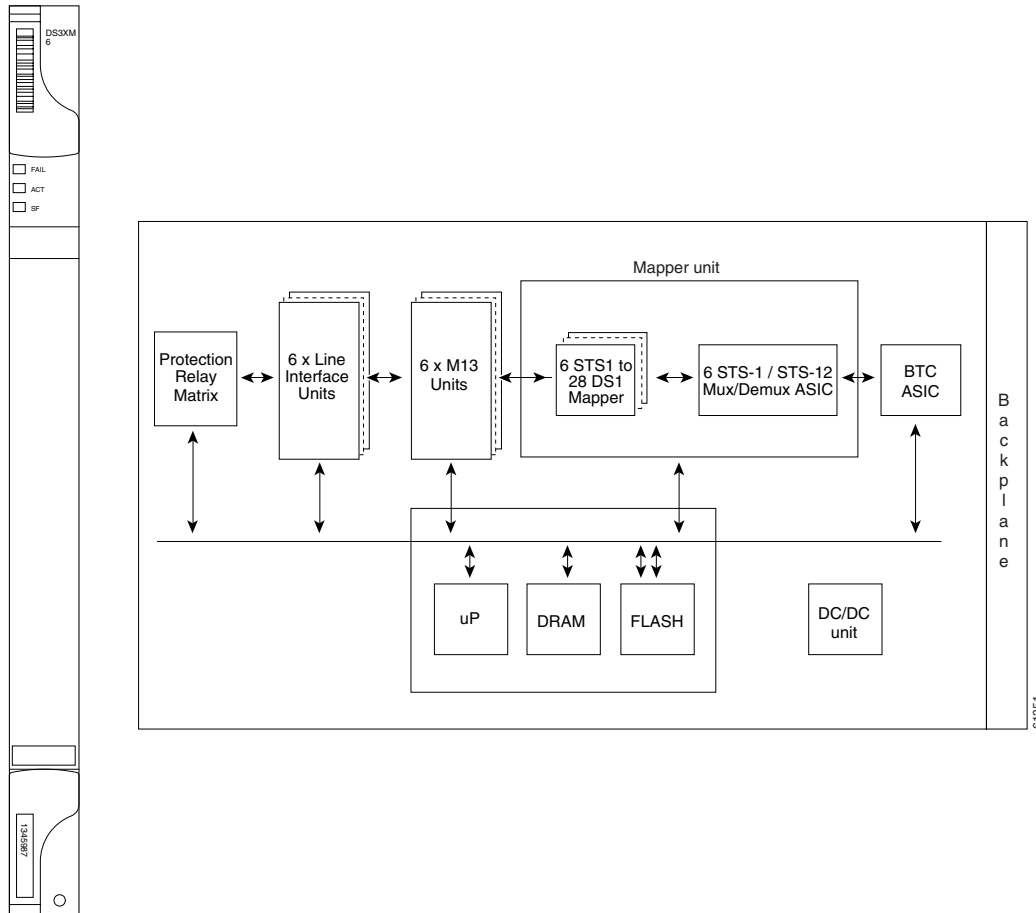
Note   You cannot create circuits from a DS3XM-6 card to a DS-3 card. DS3XM-6 cards operate at the VT1.5 level.

You can install the DS3XM-6 in any multispeed or high-speed card slot. Each DS3XM-6 port features DSX-level outputs supporting distances up to 450 feet depending on facility conditions. The DS3XM-6 card supports 1:1 protection with the proper backplane EIA. EIAs are available with BNC or SMB connectors.

4.18.1 DS3XM-6 Hosted By XCVT

The DS3XM-6 card works in conjunction with the XCVT card. A single DS3XM-6 can demultiplex (map down to a lower rate) six DS-3 signals into 168 VT1.5s that the XCVT card then manages and cross connects. XCVT cards host a maximum of 336 bidirectional VT1.5s or two DS3XM-6 cards. In most network configurations two DS3XM-6 cards are paired together as working and protect cards.

4.18.2 DS3XM-6 Card-Level Indicators

The DS3XM-6 card faceplate has three LEDs.

Table 4-29   DS3XM-6 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	When the ACTV/STBY LED is green, the DS3XM-6 card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the DS3XM-6 card is operational and in standby in a 1:1 protection group.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, or high BER on one or more of the card's ports.

4.18.3 DS3XM-6 Port-Level Indicators

You can find the status of the six DS3XM-6 card ports using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

4.18.4 DS3XM-6 Card Specifications

- DS3XM-6 Input
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
- AIS: TR-TSY-000191-compliant
  - DS3XM-6 Output
  - Bit Rate: 44.736 Mbps +/- 20 ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RG-59, 728A/Max 79 ft. RG-179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm

- – Pulse Shape: ANSI T1.102-1988 Figure 8

- – Pulse Amplitude: 0.36 - 0.85 V peak-to-peak

- – Loopback Modes: Terminal and Facility

- – Line Build Out: 0-225 ft.; 226-450 ft.

- • DS3XM-6 Electrical Interface

  - – Connectors: BNC or SMB

- • Environmental

  - – Operating Temperature:

    C-Temp (15454-DS3XM-6): 0 to +55 degrees Celsius

    I-Temp (15454-DS3XM-6-T): -40 to +65 degrees Celsius

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 20 W, 0.42 amps, 68 BTU/Hr.

- • Dimensions

  - – Height: 12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 1.8 lbs, 0.8 kg

- • Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.19 OC3 IR 4/STM1 SH 1310 Card

The OC3 IR 4/STM1 SH 1310 card provides four intermediate or short range SONET/SDH OC-3 ports compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-253. Each port operates at 155.52 Mbps over a single-mode fiber span. The card supports VT and non-concatenated or concatenated payloads at the STS-1 or STS-3c signal levels. Figure 4-21 shows the OC3 IR 4/STM1 SH 1310 faceplate and a diagram of the card.

Note The OC3 IR 4 SH 1310 and OC3 IR 4/STM1 SH 1310 cards are functionally the same.

Figure 4-21   OC3 IR 4/STM1 SH 1310 faceplate and block diagram
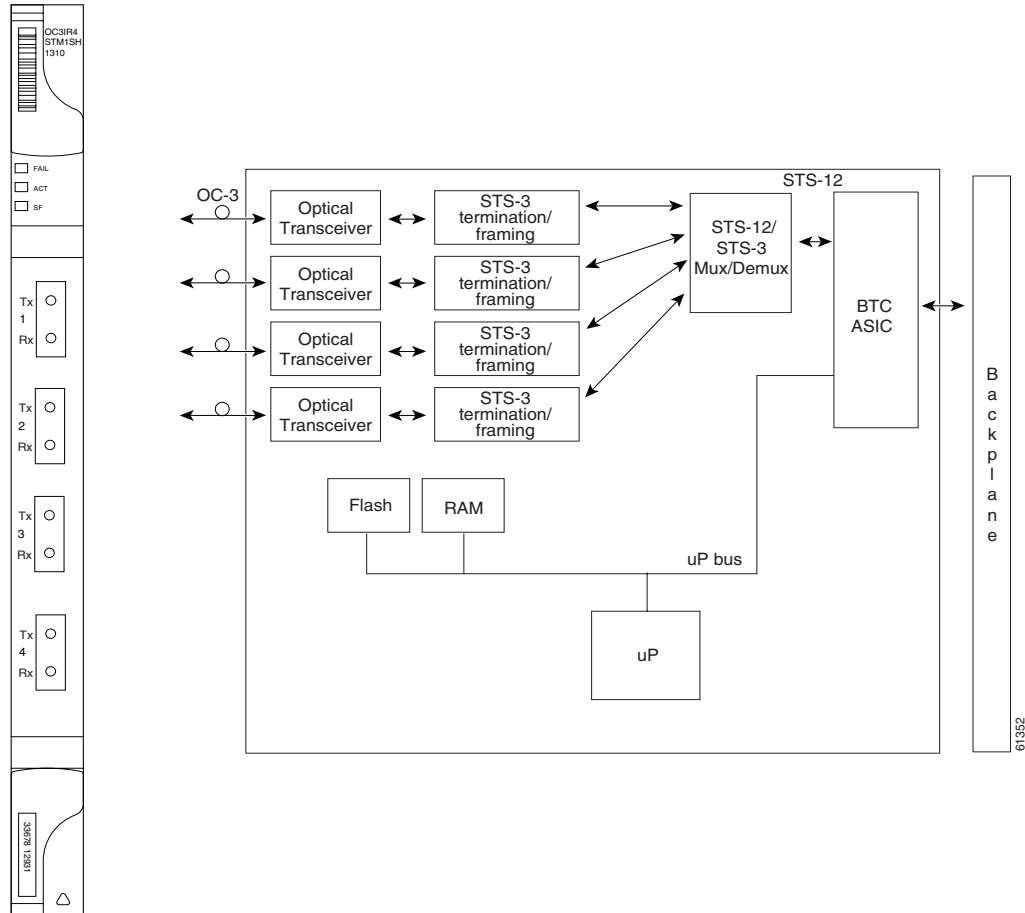
You can install the OC3 IR 4/STM1 SH 1310 card in any multispeed or high-speed card slot. The card can be provisioned as part of a unidirectional path switched ring (UPSR) or in a linear add-drop multiplexer (ADM) configuration. Each port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors.

The OC3 IR 4/STM1 SH 1310 card supports 1+1 unidirectional or bidirectional protection switching. You can provision protection on a per port basis. See the "Optical Card Protection" section on page 4-15, for more information.

The OC3 IR 4/STM1 SH 1310 detects LOS, LOF, Loss of Pointer (LOP), line Alarm Indication Signal (AIS-L), and line Remote Defect Indication (RDI-L) conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line bit interleaved parity (BIP) errors.

4.19.1 OC3 IR 4/STM1 SH 1310 Card-Level Indicators

The OC3 IR 4/STM1 SH 1310 card has three card-level LED indicators.

Table 4-30   OC3 IR 4/STM1 SH 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. 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.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BER on one or more of the card's ports. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.19.2 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 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

## 4.19.3 OC3 IR 4/STM1 SH 1310 Card Specifications

- Line
  - Bit Rate:155.52 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connector: SC
  - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.707, ITU-T G.957
  - Transmitter
  - Max. Transmitter Output Power: -8 dBm
  - Min. Transmitter Output Power: -15 dBm
  - Center Wavelength: 1274 nm – 1356 nm
  - Nominal Wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Max. Receiver Level: -8 dBm

- – Min. Receiver Level: -28 dBm
- – Receiver: InGaAs/InP photo detector
- – Link Loss Budget: 13 dB
- Environmental
  - – Operating Temperature:

    C-Temp (15454-OC34IR1310): 0 to +55 degrees Celsius

    I-Temp (15454-OC34I13-T): -40 to +65 degrees Celsius
  - – Operating Humidity: 5 - 95%, non-condensing
  - – Power Consumption: 19.20 W, 0.40 amps, 65.56 BTU/Hr.
- Dimensions
  - – Height: 12.650 in.
  - – Width: 0.716 in.
  - – Depth: 9.000 in.
  - – Card Weight: 1.0 lbs, 0.4 kg
- Compliance
  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
  - – Eye Safety Compliance: Class I

4.20 OC12 IR/STM4 SH 1310 Card

The OC12 IR/STM4 SH 1310 card provides one intermediate or short range SONET/SDH OC-12 port compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-253. The port operates at 622.08 Mbps over a single-mode fiber span. The card supports VT and non-concatenated or concatenated payloads at STS-1, STS-3c, STS-6c or STS-12c signal levels. Figure 4-22 shows the OC12 IR/STM4 SH 1310 faceplate and a block diagram of the card.

Note   The OC12 IR 1310 and OC12/STM4 SH 1310 cards are functionally the same.

Figure 4-22   OC12 IR/STM4 SH 1310 faceplate and block diagram
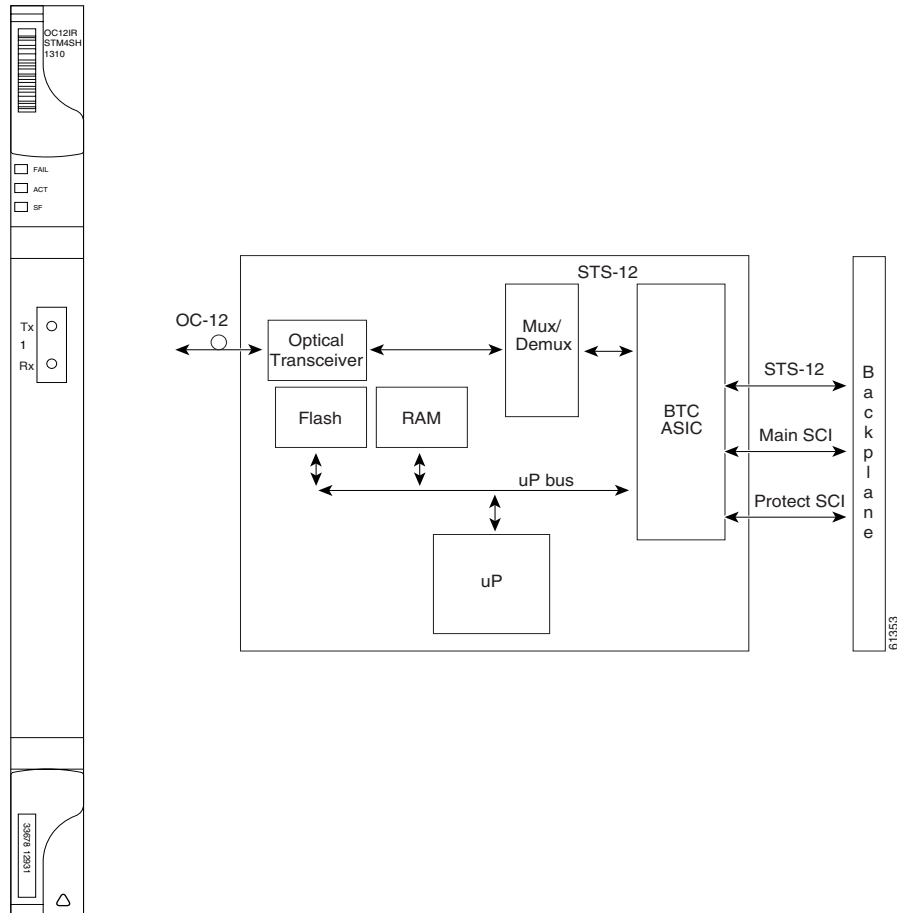
You can install the OC12 IR/STM4 SH 1310 card in any multispeed or high-speed card slot and provision the card as a drop card or span card in a two-fiber BLSR, UPSR, or in ADM (linear) configurations.

The OC12 IR/STM4 SH 1310 port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 IR/STM4 SH 1310 uses SC optical connections and supports 1+1 unidirectional and bidirectional protection.

The OC12 IR/STM4 SH 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card counts section and line BIT errors.

4.20.1 OC12 IR/STM4 SH 1310 Card-Level Indicators

The OC12 IR/STM4 SH 1310 card has three card-level LED indicators.

Table 4-31   OC12 IR/STM4 SH 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. 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.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.20.2 OC12 IR/STM4 SH 1310 Port-Level Indicators

You can find the status of the OC-12 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

# 4.20.3 OC12 IR/STM4 SH 1310 Card Specifications

- Line
  - Bit Rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.707, ITU-T G.957
- Transmitter
  - Max. Transmitter Output Power: -8 dBm
  - Min. Transmitter Output Power: -15 dBm
  - Center Wavelength: 1274 nm – 1356 nm
  - Nominal Wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Max. Receiver Level: -8 dBm

- – Min. Receiver Level: -28 dBm
- – Receiver: InGa As/InP photo detector
- – Link Loss Budget: 13 dB
- Environmental
  - – Operating Temperature:

    C-Temp (15454-OC121IR1310): 0 to +55 degrees Celsius

    I-Temp (15454-OC121I13-T): -40 to +65 degrees Celsius
  - – Operating Humidity: 5 - 95%, non-condensing
  - – Power Consumption: 10.90 W, 0.23 amps, 37.22 BTU/Hr.
- Dimensions
  - – Height: 12.650 in.
  - – Width: 0.716 in.
  - – Depth: 9.000 in.
  - – Card Weight: 1.4 lbs, 0.6 kg
- Compliance
  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
  - – Eye Safety Compliance: Class I

4.21 OC12 LR/STM4 LH 1310 Card

The OC12 LR/STM4 LH 1310 card provides one long-range, ITU-T G.707, ITU-T G.957, and Telcordia-compliant, GR-253 SONET OC-12 port per card. The port operates at 622.08 Mbps over a single-mode fiber span. The card supports VT and non-concatenated or concatenated payloads at STS-1, STS-3c, STS-6c or STS-12c signal levels. Figure 4-23 shows the OC12 LR/STM4 LH 1310 faceplate and a block diagram of the card.

Note   The OC12 LR 1310 and OC12 LR/STM4 LH 1310 cards are functionally the same.

Figure 4-23   OC12 LR/STM4 LH 1310 faceplate and block diagram
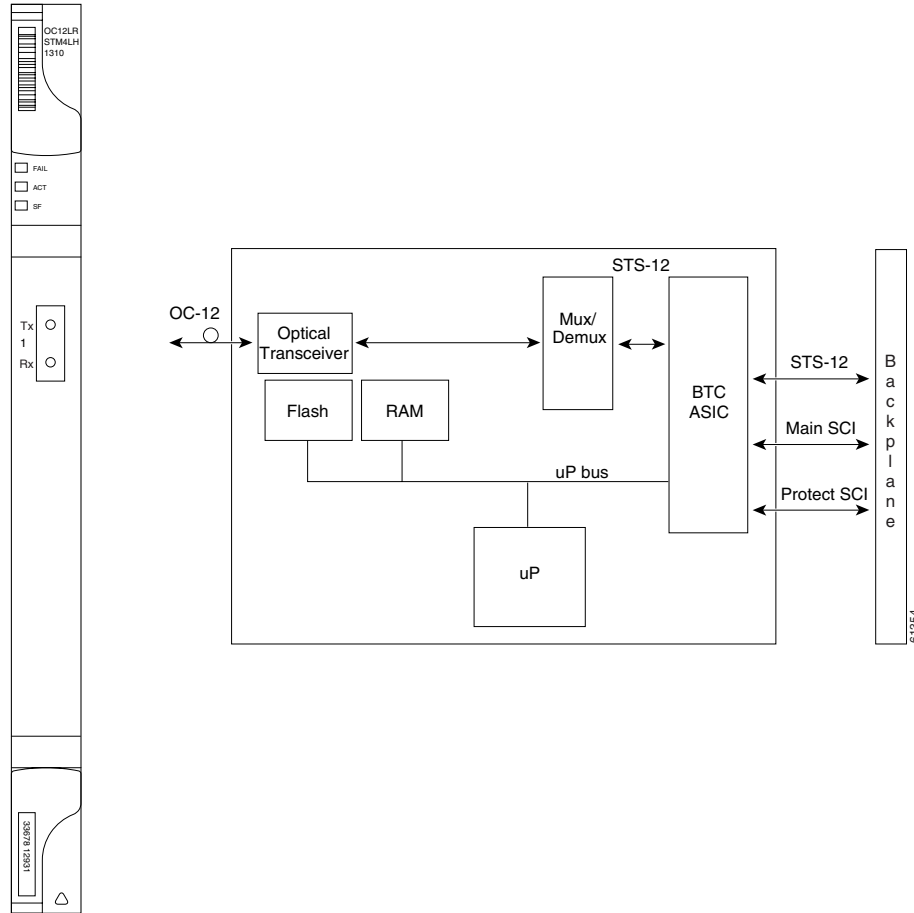
You can install the OC12 LR/STM4 LH 1310 card in any multispeed or high-speed card slot and provision the card as a drop card or span card in a two-fiber BLSR (Bidirectional line switched ring), UPSR, or ADM (linear) configuration.

The OC12 LR/STM4 LH 1310 card port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC optical connections supporting 1+1 unidirectional and bidirectional protection.

The OC12 LR/STM4 LH 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.21.1 OC12 LR/STM4 LH 1310 Card-Level Indicators

The OC12 LR/STM4 LH 1310 card has three card-level LED indicators.

Table 4-32   OC12 LR/STM4 LH 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
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.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.21.2 OC12 LR/STM4 LH 1310 Port-Level Indicators

You can find the status of the OC12 LR/STM4 LH 1310 card port using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.21.3 OC12 LR/STM4 LH 1310 Card Specifications

- Line
  - Bit Rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-253-CORE, ITU-T G.707, ITU-T G.957
- Transmitter
  - Max. Transmitter Output Power: +2 dBm
  - Min. Transmitter Output Power: -3 dBm
  - Center Wavelength: 1280 nm – 1335 nm
  - Nominal Wavelength: 1310 nm
  - Transmitter: Distributed feedback laser
- Receiver
  - Max. Receiver Level: -8 dBm

- – Min. Receiver Level: -28 dBm
- – Receiver: InGaAs/InP photo detector
- – Link Loss Budget: 25 dB
- Environmental
  - – Operating Temperature:

    C-Temp (15454-OC121LR1310): 0 to +55 degrees Celsius

    I-Temp (15454-OC121L13-T): -40 to +65 degrees Celsius
  - – Operating Humidity: 5 - 95%, non-condensing
  - – Power Consumption: 12 W, 0.25 amps, 41BTU/Hr.
- Dimensions
  - – Height: 12.650 in.
  - – Width: 0.716 in.
  - – Depth: 9.000 in.
  - – Card Weight: 1.4 lbs, 0.6 kg
- Compliance
  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
  - – Eye Safety Compliance: Class I

4.22 OC12 LR/STM4 LH 1550 Card

The OC12 LR/STM4 LH 1550 card provides one long-range SONET/SDH OC-12 port compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-253. The port operates at 622.08 Mbps over a single-mode fiber span. The card supports VT and non-concatenated, or concatenated payloads at STS-1, STS-3c, STS-6c, or STS-12c signal levels. Figure 4-24 shows the OC12 LR/STM4 LH 1550 faceplate and a block diagram of the card.

Note   The OC12 LR 1550 and OC12 LR/STM4 LH 1550 cards are functionally the same.

Figure 4-24   OC12 LR/STM4 LH 1550 faceplate and block diagram
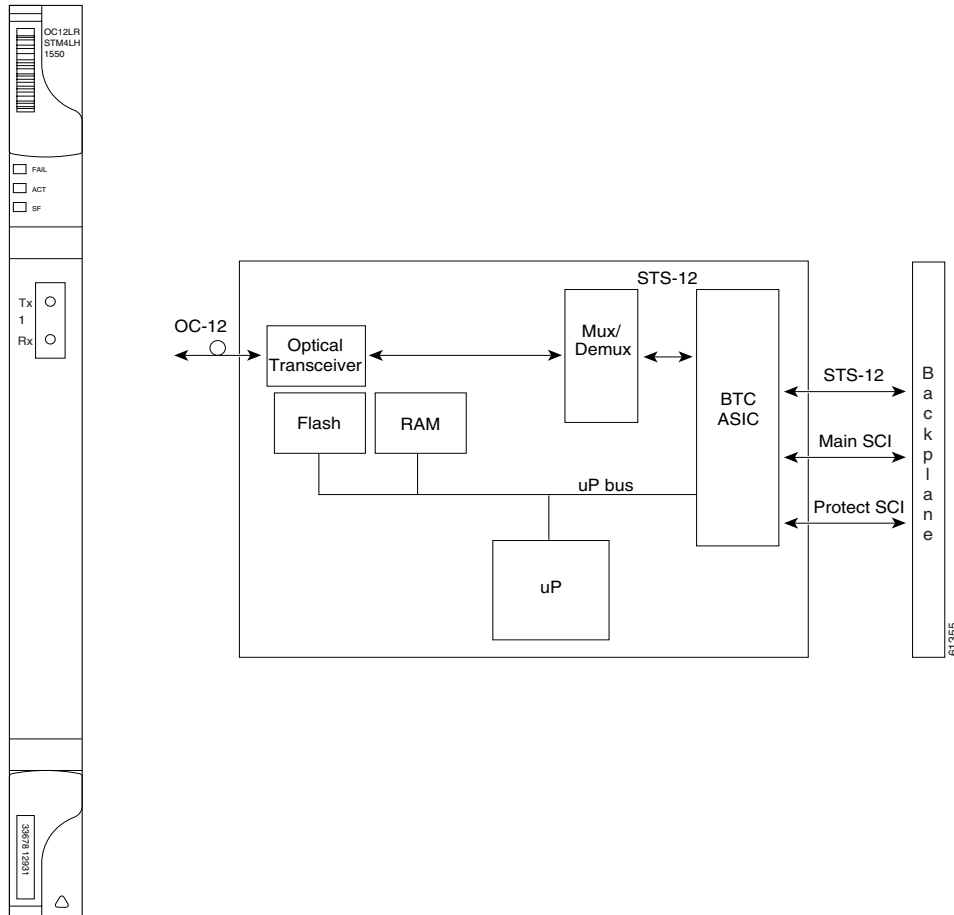
You can install the OC12 LR/STM4 LH 1550 card in any multispeed card slot. The OC12 LR/STM4 LH 1550 can be provisioned as part of a two-fiber BLSR, UPSR or linear ADM.

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, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.22.1 OC12 LR/STM4 LH 1550 Card-Level Indicators

The OC12 LR/STM4 LH 1550 card has three card-level LED indicators.

Table 4-33   OC12 LR/STM4 LH 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC12 LR/STM4 LH 1550 card is operational and ready to carry traffic.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.22.2 OC12 LR/STM4 LH 1550 Port-Level Indicators

You can find the status of the OC12 LR/STM4 LH 1550 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

## 4.22.3 OC12 LR/STM4 LH 1550 Card Specifications

- Line
  - Bit Rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-253-CORE, ITU-T G.707, ITU-T G.957
- Transmitter
  - Max. Transmitter Output Power: +2 dBm
  - Min. Transmitter Output Power: -3 dBm
  - Center Wavelength: 1480 nm – 1580 nm
  - Nominal Wavelength: 1550 nm
  - Transmitter: Distributed feedback laser
- Receiver
  - Max. Receiver Level: -8 dBm

  – Min. Receiver Level: -28 dBm

  – Receiver: InGaAs/InP photo detector

  – Link Loss Budget: 25 dB

- Environmental

  – Operating Temperature:

  C-Temp (15454-OC121LR1550): 0 to +55 degrees Celsius

  I-Temp (15454-OC121L15-T): -40 to +65 degrees Celsius

  – Operating Humidity: 5 - 95%, non-condensing

  – Power Consumption: 9.28 W, 0.19 amps, 31.68 BTU/Hr.

- Dimensions

  – Height: 12.650 in.

  – Width: 0.716 in.

  – Depth: 9.000 in.

  – Card Weight: 1.4 lbs, 0.6 kg

- Compliance

  – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  – Eye Safety Compliance: Class I

4.23 OC48 IR 1310 Card

The OC48 IR 1310 card provides one intermediate-range, Telcordia-compliant, GR-253 SONET OC-48 port per card. Each port operates at 2.49 Gbps over a single-mode fiber span. The card supports VT and non-concatenated, or concatenated payloads at STS-1, STS-3c, STS-6c, STS-12c, or STS-48c signal levels. Figure 4-25 shows the OC48 IR 1310 faceplate and a block diagram of the card.

Figure 4-25   OC48 IR 1310 faceplate and block diagram
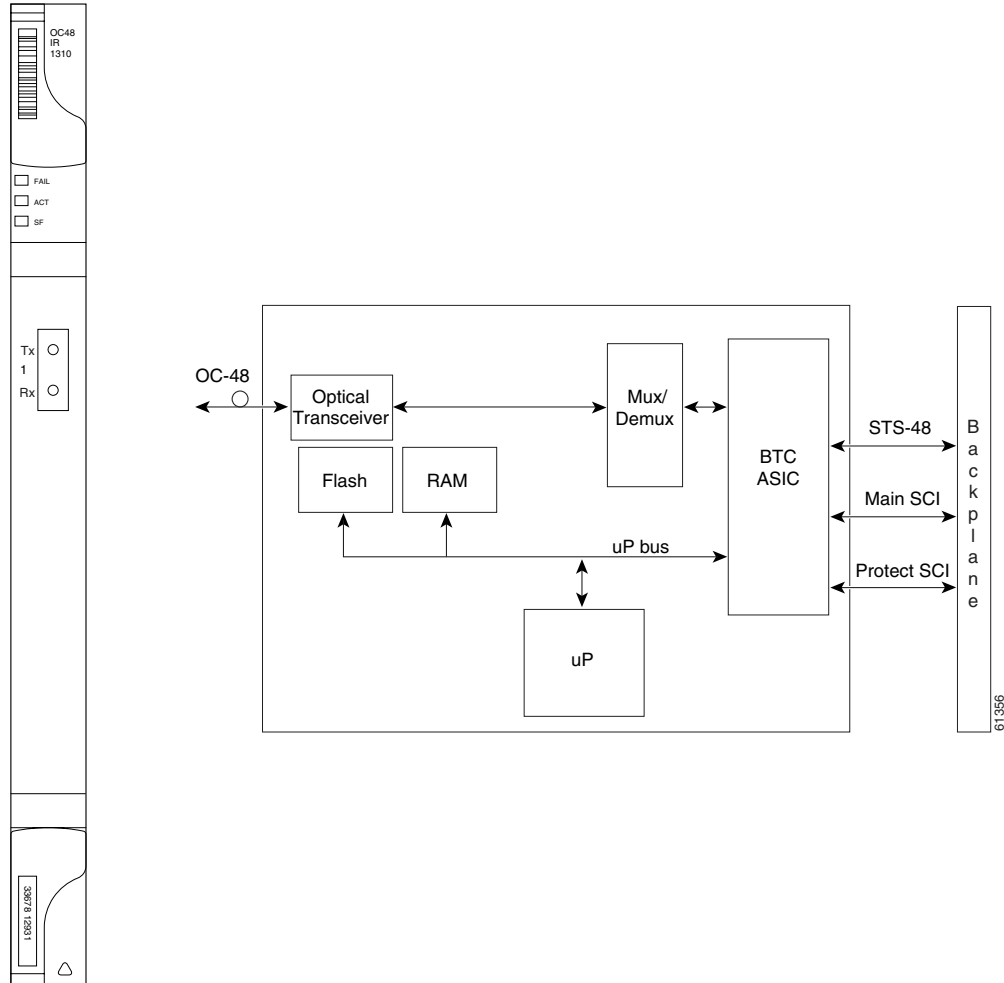
You can install the OC48 IR 1310 card in any high-speed card slot and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration.

The OC-48 port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC48 IR 1310 uses SC connectors. The card supports 1+1 unidirectional and bidirectional protection switching.

The OC48 IR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.23.1 OC48 IR 1310 Card-Level Indicators

The OC48 IR 1310 card has three card-level LED indicators.

Table 4-34   OC48 IR 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 IR 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.23.2 OC48 IR 1310 Port-Level Indicators

You can find the status of the OC48 IR 1310 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.23.3 OC48 IR 1310 Card Specifications

- Line
  - Bit Rate: 2.49 Gbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Max. Transmitter Output Power: 0 dBm
  - Min. Transmitter Output Power: -5 dBm
  - Center Wavelength: 1280 nm – 1350 nm
 - Nominal Wavelength: 1310 nm

    Transmitter: Uncooled direct modulated DFB
- Receiver
  - Max. Receiver Level: 0 dBm

- – Min. Receiver Level: -18 dBm

  – Receiver: InGaAs InP photo detector

  – Link Loss Budget: 13 dB min.

- Environmental

  – Operating Temperature:

    C-Temp (15454-OC481IR1310): 0 to +55 degrees Celsius

  – Operating Humidity: 5 - 95%, non-condensing

  – Power Consumption: 32.20 W, 0.67 amps, 109.94 BTU/Hr.

- Dimensions

  – Height: 12.650 in.

  – Width: 0.716 in.

  – Depth: 9.000 in.

  – Card Weight: 1.8 lbs, 0.8 kg

- Compliance

  – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  – Eye Safety Compliance: Class I

4.24 OC48 LR 1550 Card

The OC48 LR 1550 card provides one long-range, Telcordia-compliant, GR-253 SONET OC-48 port per card. Each port operates at 2.49 Gbps over a single-mode fiber span. The card supports VT, non-concatenated or concatenated payloads at STS-1, STS-3c, STS-6c STS-12c or STS-48c signal levels. Figure 4-26 shows the OC48 LR 1550 faceplate and a block diagram of the card.

Figure 4-26   OC48 LR 1550 faceplate and block diagram
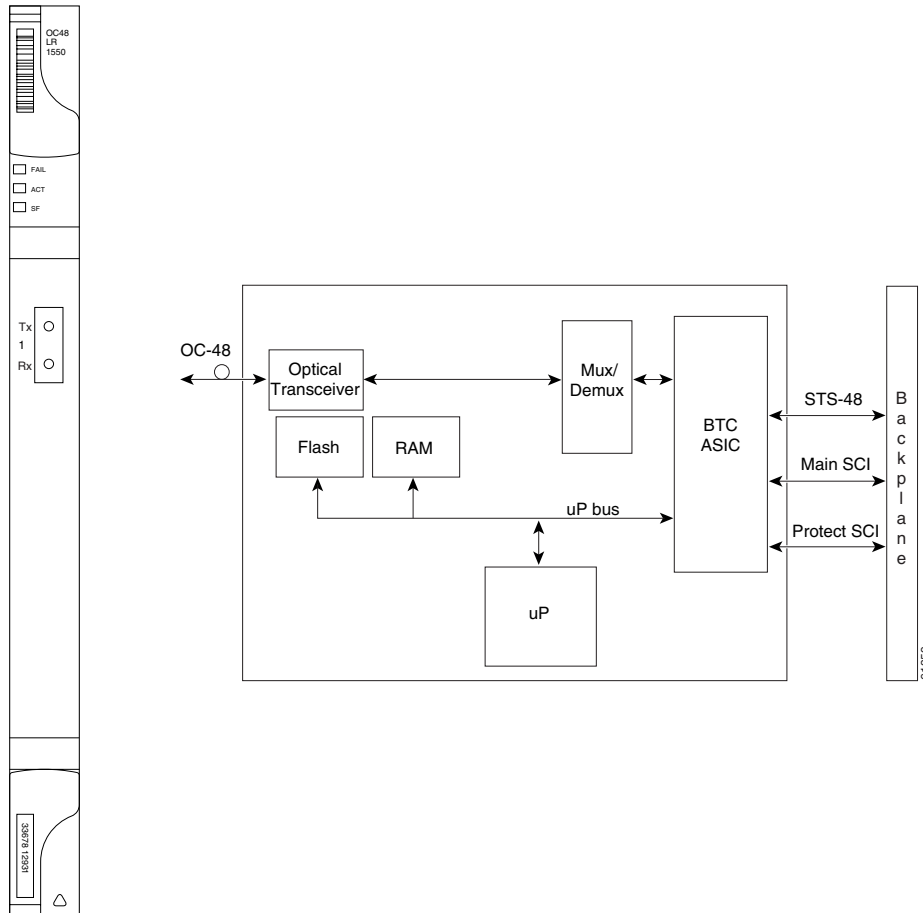
You can install OC48 LR 1550 cards in any high-speed slot on the ONS 15454 and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration.

The OC48 LR 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 and bidirectional protection switching.

The OC48 LR 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.24.1 OC48 LR 1550 Card-Level Indicators

The OC48 LR 1550 card has three card-level LED indicators.

Table 4-35   OC48 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.24.2 OC48 LR 1550 Port-Level Indicators

You can find the status of the OC48 LR 1550 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.24.3 OC48 LR 1550 Card Specifications

- Line
  - Bit Rate: 2.49 Gbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Max. Transmitter Output Power: +3 dBm
  - Min. Transmitter Output Power: -2 dBm
  - Center Wavelength: 1520 nm – 1580 nm
  - Nominal Wavelength: 1550 nm
  - Transmitter: Distributed feedback laser
- Receiver
  - Max. Receiver Level: -8 dBm

- – Min. Receiver Level: -28 dBm

- – Receiver: InGaAs APD photo detector

- – Link Loss Budget: 26 dB min., with 1 dB dispersion penalty

- Environmental

  - – Operating Temperature:

    C-Temp (15454-OC481LR1550): 0 to +55 degrees Celsius

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 26.80 W, 0.56 amps, 91.50 BTU/Hr.

- Dimensions

  - – Height:12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 1.8 lbs, 0.8 kg

- Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  - – Eye Safety Compliance: Class I

4.25 OC48 IR/STM16 SH AS 1310 Card

The OC48 IR/STM16 SH AS 1310 card provides one intermediate-range SONET/SDH OC-48 port compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-253. The port operates at 2.49 Gbps over a single-mode fiber span. The card supports VT and non-concatenated or concatenated payloads at STS-1, STS-3c, STS-6c, STS-12c, or STS-48c signal levels. Figure 4-27 shows the OC48 IR/STM16 SH AS 1310 faceplate and a block diagram of the card.

Figure 4-27   OC48 IR/STM16 SH AS 1310 faceplate and block diagram
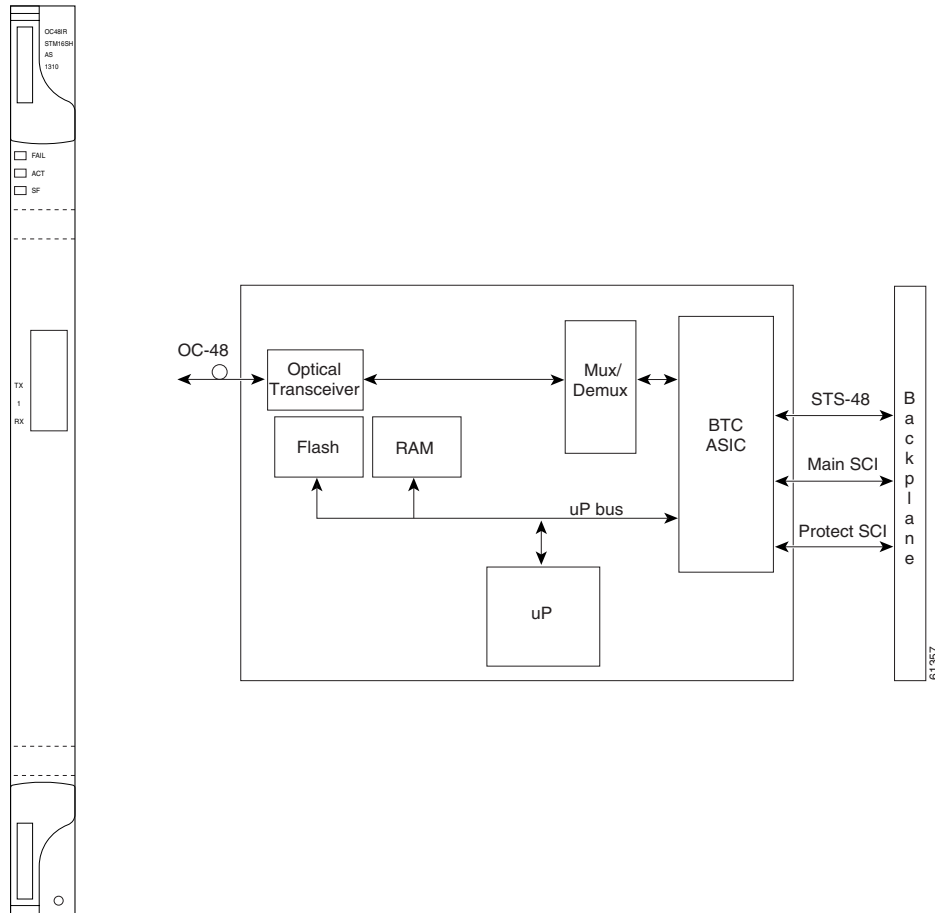
You can install the OC48 IR/STM16 SH AS 1310 card in any multispeed or high-speed card slot on the ONS 15454 and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration.

The OC-48 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 and bidirectional protection switching.

The OC48 IR/STM16 SH AS 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.25.1 OC48 IR/STM16 SH AS 1310 Card-Level Indicators

The OC48 IR/STM16 SH AS 1310 card has three card-level LED indicators.

Table 4-36   OC48 IR/STM16 SH AS 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 IR/STM16 SH AS 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.25.2 OC48 IR/STM16 SH AS 1310 Port-Level Indicators

You can find the status of the OC48 IR/STM16 SH AS 1310 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.25.3 OC48 IR/STM16 SH AS 1310 Compatibility

Use the XC10G card, the TCC+ card, the new 15454-SA-ANSI shelf assembly, and Software R3.1 or higher to enable the OC48 IR/STM16 SH AS 1310 card. The OC48 IR/STM16 SH AS 1310 card uses the BTC backplane interface to provide recognition in both the high-speed and multispeed slots.

4.25.4 OC48 IR/STM16 SH AS 1310 Card Specifications

- Line
  - Bit Rate: 2.49 Gbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm Single Mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.707, ITU-T G.957
- Transmitter
  - Max. Transmitter Output Power: 0 dBm
  - Min. Transmitter Output Power: -5 dBm

- – Center Wavelength: 1280 nm – 1350 nm

- – Nominal Wavelength: 1310nm

- – Transmitter: Distributed feedback laser

- • Receiver

  - – Max. Receiver Level: 0 dBm

  - – Min. Receiver Level: -18 dBm

  - – Receiver: InGaAs InP photo detector

  - – Link Loss Budget: 13 dB min.

- • Environmental

  - – Operating Temperature:

    C-Temp (15454-OC481IR1310A): 0 to +55 degrees Celsius

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 37.20 W, 0.77 amps, 127.01 BTU/Hr.

- • Dimensions

  - – Height: 12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 2.2 lbs, 0.9 kg

- • Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  - – Eye Safety Compliance: Class I

4.26 OC48 LR/STM16 LH AS 1550 Card

The OC48 LR/STM16 LH AS 1550 card provides one long-range SONET/SDH OC-48 port compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-253. Each port operates at 2.49 Gbps over a single-mode fiber span. The card supports VT and non-concatenated or concatenated payloads at STS-1, STS-3c, STS-6c, STS-12c, or STS-48c signal levels. Figure 4-28 shows the OC48 LR/STM16 LH AS 1550 faceplate and a block diagram of the card.

Figure 4-28   OC48 LR/STM16 LH AS 1550 faceplate and block diagram
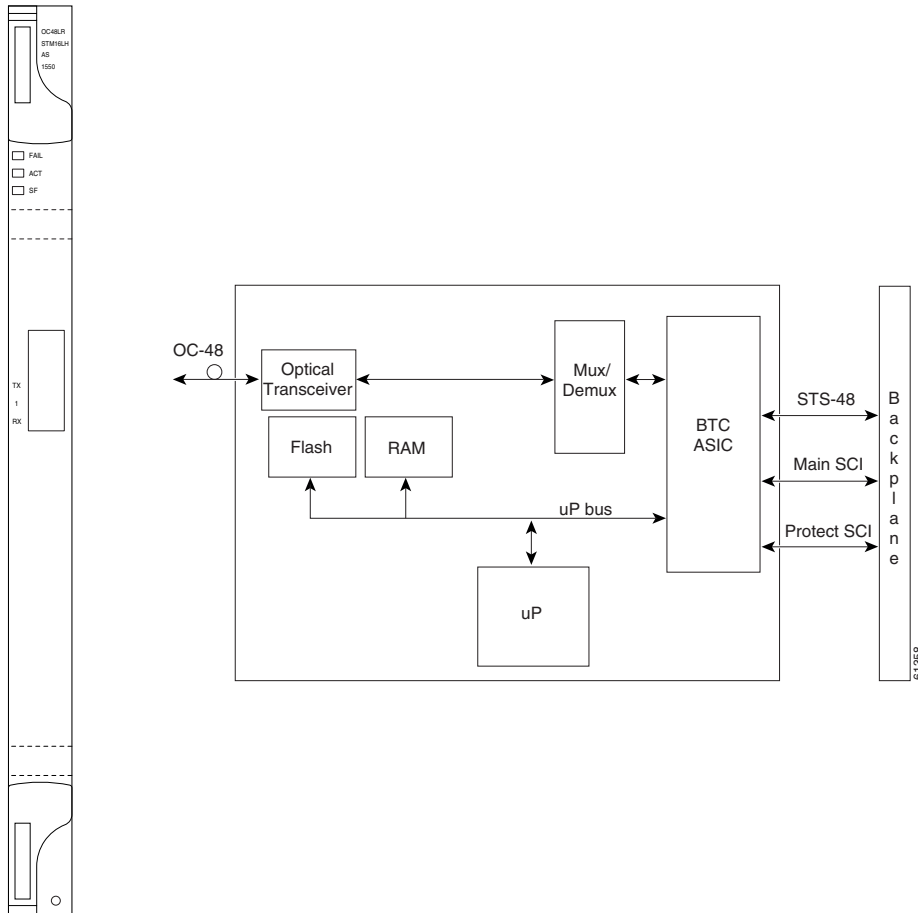
You can install OC48 LR/STM16 LH AS 1550 cards in any multispeed or high-speed slot on the ONS 15454 and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration.

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 and bidirectional protection switching.

The OC48 LR/STM16 LH AS 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors.

4.26.1 OC48 LR/STM16 LH AS 1550 Card-Level Indicators

The OC48 LR/STM16 LH AS 1550 card has three card-level LED indicators.

Table 4-37   OC48 LR/STM16 LH AS 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 LR/STM16 LH AS 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.26.2 OC48 LR/STM16 LH AS 1550 Port-Level Indicators

You can find the status of the OC48 LR/STM16 LH AS 1550 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

⚠️
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.**

4.26.3 OC48 LR/STM16 LH AS 1550 Compatibility

Use the XC10G card, the TCC+ card, the new 15454-SA-ANSI shelf assembly, and Software R3.1 or higher to enable the OC48 LR/STM16 LH AS 1550 card. The OC48 LR/STM16 LH AS 1550 card uses the BTC backplane interface to provide recognition in both the high-speed and multispeed slots.

4.26.4 OC48 LR/STM16 LH AS 1550 Card Specifications

- Line
    - Bit Rate: 2.49 Gbps
    - Code: Scrambled NRZ
    - Fiber: 1550 nm Single Mode
    - Loopback Modes: Terminal and Facility
    - Connectors: SC
    - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.707, ITU-T G.957
- Transmitter
    - Max. Transmitter Output Power: +3 dBm
    - Min. Transmitter Output Power: -2 dBm

- – Center Wavelength: 1520 nm – 1580 nm

  – Nominal Wavelength: 1550 nm

  – Transmitter: Distributed feedback laser

- Receiver

  – Max. Receiver Level: -8 dBm

  – Min. Receiver Level: -28 dBm

  – Receiver: InGaAs APD photo detector

  – Link Loss Budget: 26 dB min., with 1 dB dispersion penalty

- Environmental

  – Operating Temperature:

    C-Temp (15454-OC481LR1550A): 0 to +55 degrees Celsius

  – Operating Humidity: 5 - 95%, non-condensing

  – Power Consumption: 37.20 W, 0.77 amps, 127.01 BTU/Hr.

- Dimensions

  – Height:12.650 in.

  – Width: 0.716 in.

  – Depth: 9.000 in.

  – Card Weight: 2.2 lbs, 0.9 kg

- Compliance

  – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  – Eye Safety Compliance: Class I

4.27 OC48 ELR/STM16 EH 100 GHz Cards

Thirty-seven distinct OC48 ITU 100GHz dense wavelength division multiplexing (DWDM) cards provide the ONS 15454 DWDM channel plan. Each OC-48 DWDM card has one SONET OC-48/SDH STM-16 port that complies with Telcordia, GR-253 SONET, and the International Telecommunication Union's ITU-T G.692, and ITU-T G.958.

The port operates at 2.49 Gbps over a single-mode fiber span. The card carries VT, concatenated, and non-concatenated payloads at STS-1, STS-3c, STS-6c, STS-12c, or STS-48c signal levels. Figure 4-29 shows the OC48 ELR/STM16 EH 100 GHz faceplate and a block diagram of the card.

Figure 4-29   OC48 ELR/STM16 EH 100 GHz faceplate and block diagram
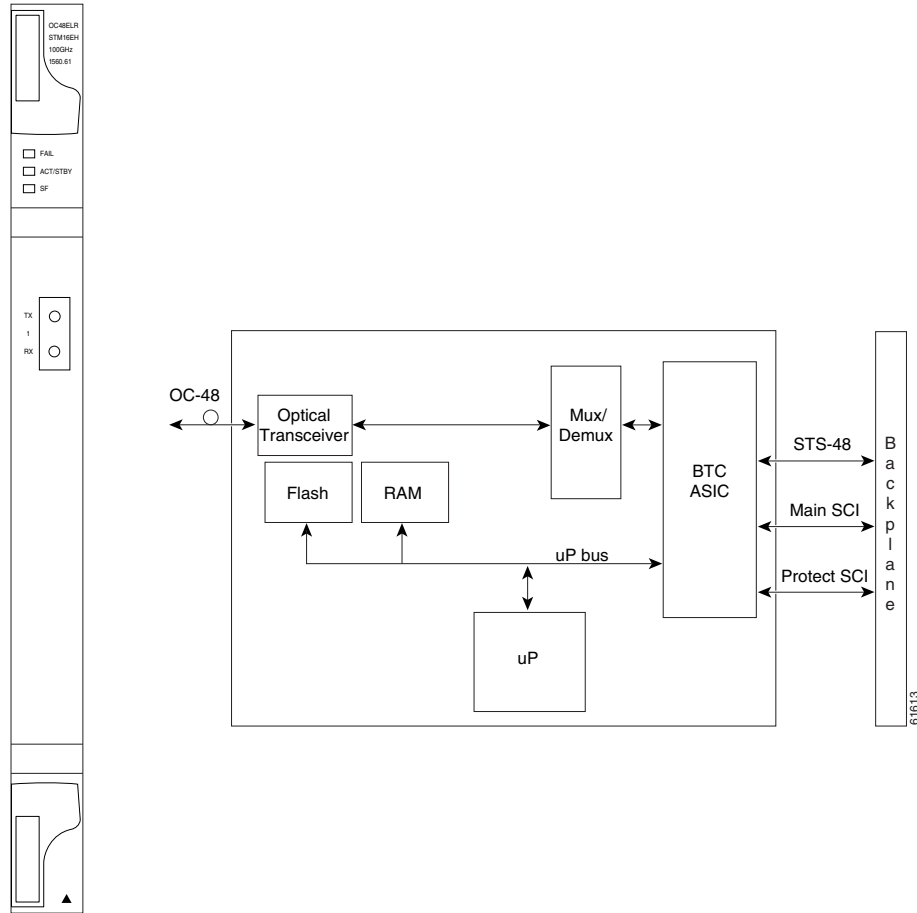
Nineteen of the cards operate in the blue band with spacing of 100 GHz on the ITU grid standard G.692 and Telcordia GR-2918-CORE, issue 2 (1528.77 nm, 1530.33 nm, 1531.12 nm, 1531.90 nm, 1532.68 nm, 1533.47 nm, 1534.25 nm, 1535.04 nm, 1535.82 nm, 1536.61 nm, 1538.19 nm, 1538.98 nm, 1539.77 nm, 1540.56 nm, 1541.35 nm, 1542.14 nm, 1542.94 nm, 1543.73 nm, 1544.53 nm).

The other eighteen cards operate in the red band with spacing of 100 GHz on the ITU grid (1546.12 nm, 1546.92 nm, 1547.72 nm, 1548.51 nm,1549.32 nm, 1550.12 nm, 1550.92 nm, 1551.72 nm, 1552.52 nm, 1554.13 nm, 1554.94 nm, 1555.75 nm, 1556.55 nm, 1557.36 nm, 1558.17 nm, 1558.98 nm, 1559.79 nm, 1560.61 nm). These cards are also designed to interoperate with the Cisco ONS 15216 DWDM solution.

You can install the OC48 ELR/STM16 EH 100 GHz cards in any high-speed slot and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration. Each OC48 ELR/STM16 EH 100 GHz card uses extended long reach optics operating individually within the ITU-T 100 GHz grid. The OC-48 DWDM 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 Cisco ONS 15216 erbium-doped fiber amplifiers (EDFAs).

Maximum system reach in filterless applications is 26 dB 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. When used in combination with ONS 15216 100 GHz filters, the link budget is reduced by the insertion loss of the filters plus an additional 2dB

power penalty. The OC-48 ELR DWDM cards wavelength stability is +/- 0.12 nm for the life of the product and over the full range of operating temperatures. Each interface contains a transmitter and receiver.

The OC-48 ELR cards detect loss of signal (LOS), loss of frame (LOF), loss of pointer (LOP), and line-layer alarm indication signal (AIS-L) conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The cards also count section and line BIT errors.

4.27.1 OC48 ELR 100 GHz Card-Level Indicators

The OC48 ELR/STM16 EH 100 GHz cards have three card-level LED indicators.

Table 4-38   OC48 ELR/STM16 EH 100 GHz Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 ELR card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.27.2 OC48 ELR 100 GHz Port-Level Indicators

You can find the status of the OC48 ELR card ports using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.27.3 OC48 ELR 100 GHz Compatibility

The OC48 ELR/STM16 EH 100 GHz card requires a cross-connect (XC) card, cross-connect virtual tributary (XCVT) card, or an XC10G for proper operation.

4.27.4 OC48 ELR 100 GHz Card Specifications

- Line
  - Bit Rate: 2.49 Gbps

- – Code: Scrambled NRZ

- – Fiber: 1550 nm single-mode

- – Loopback Modes: Terminal and Facility

- – Connectors: SC

- – Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.692, ITU-T G.958

- Transmitter

  - – Max. Transmitter Output Power: 0 dBm

  - – Min. Transmitter Output Power: -2 dBm

  - – Center Wavelength: ±.12 nm

  - – Transmitter: Electro-absorption laser

- Receiver

  - – Max. Receiver Level: -9 dBm

  - – Min. Receiver Level: -27 dBm at 1E-12 BER

  - – Receiver: InGaAs APD photo detector

  - – Link Loss Budget: 25 dB min. at BER=10E-12, (not including the power dispersion penalty)

  - – Dispersion Penalty: 2dB for a dispersion of up to 5400 ps/nm

- Environmental

  - – Operating Temperature:

    C-Temp: 0 to +55 degrees Celsius (For product names, see Card Temperature Ranges, page 4-6)

  - – Operating Humidity: 5 - 95%, non-condensing

  - – Power Consumption: 31.20 W, 0.65 amps, 106.53 BTU/Hr.

- Dimensions

  - – Height:12.650 in.

  - – Width: 0.716 in.

  - – Depth: 9.000 in.

  - – Card Weight: 2.4 lbs, 1.1 kg

- Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  - – Eye Safety Compliance: Class I

4.28 OC48 ELR 200 GHz Cards

Eighteen distinct OC48 ITU 200GHz dense wavelength division multiplexing (DWDM) cards provide the ONS 15454 DWDM channel plan. Each OC-48 DWDM card provides one Telcordia-compliant, GR-253 SONET OC-48 port. The port operates at 2.49 Gbps over a single-mode fiber span. The card carries VT, concatenated, and non-concatenated payloads at STS-1, STS-3c, STS-6c, STS-12c, or STS-48c signal levels. Figure 4-29 shows the OC48 ELR DWDM faceplate and a block diagram of the card.

Figure 4-30   OC48 ELR 200 GHz faceplate and block diagram
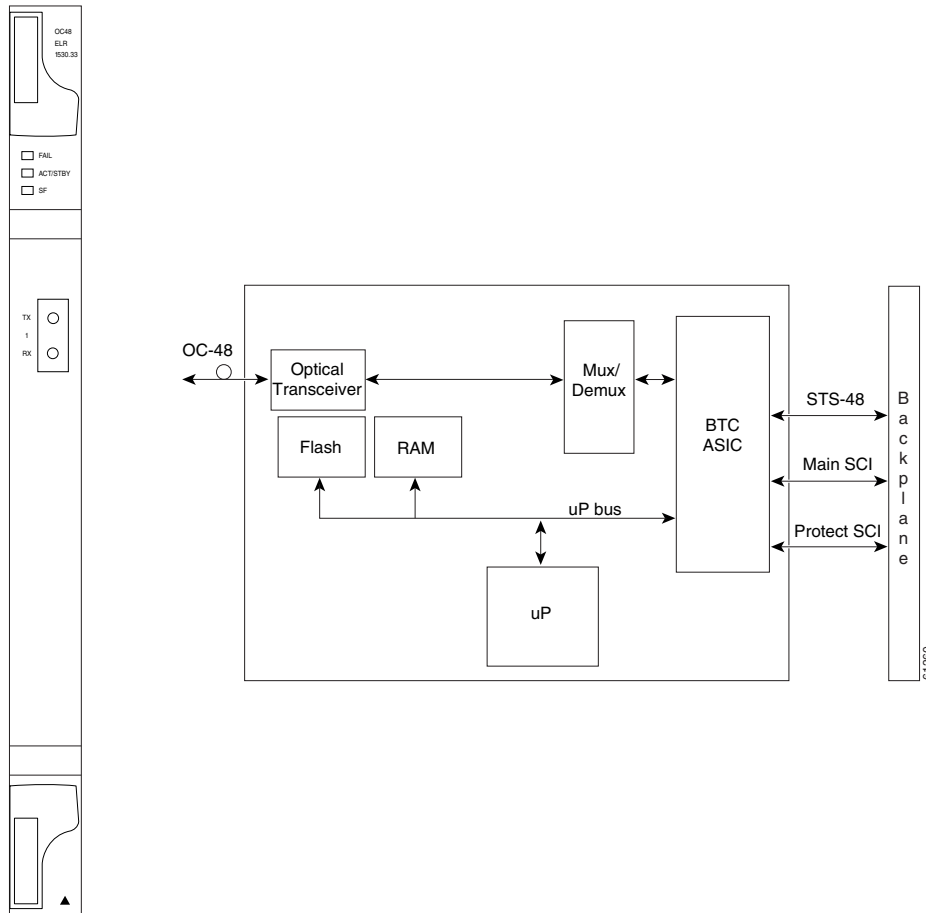
Nine of the cards operate in the blue band with spacing of 200 GHz on the ITU grid (1530.33 nm, 1531.90 nm, 1533.47 nm, 1535.04 nm, 1536.61 nm, 1538.19 nm, 1539.77 nm, 1541.35 nm, 1542.94 nm).

The other nine cards operate in the red band with spacing of 200 GHz on 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, 1560.61 nm). These cards are also designed to interoperate with the Cisco ONS 15216 DWDM solution.

You can install the OC48 ELR 200 GHz cards in any high-speed slot and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration. Each OC48 ELR DWDM card uses extended long reach optics operating individually within the ITU-T 200 GHz grid. The OC48 DWDM 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 or other performance-affecting factors. The OC48 ELR DWDM cards feature wavelength stability of +/- 0.25 nm. Each interface contains a transmitter and receiver.

The OC48 ELR DWDM cards are the first in a family of cards meant to support extended long reach applications in conjunction with optical amplification. Using electro-absorption technology, the OC48 DWDM cards provide a solution at the lower-extended long reach distances.

The OC48 LR 1550 interface features a 1550 nm 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 cards detect LOS, LOF, LOP, AIS-L, and RDI-L conditions. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The cards also count section and line BIT errors.

To enable APS, the OC48 ELR cards extract the K1 and K2 bytes from the SONET overhead. The DCC bytes are forwarded to the TCC+ card; the TCC+ terminates the DCC.

4.28.1 OC48 ELR 200 GHz Card-Level Indicators

The OC48 ELR cards have three card-level LED indicators.

Table 4-39   OC48 ELR 200 GHz Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 ELR card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.28.2 OC48 ELR 200 GHz Port-Level Indicators

You can find the status of the OC48 ELR card ports using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to quickly view the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

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.**

4.28.3 OC48 ELR 200 GHz Compatibility

The OC48 ELR/STM16 EH 200 GHz card requires an XC card, XCVT card, or XC10G card for proper operation.

4.28.4 OC48 ELR 200 GHz Card Specifications

- Line
  - Bit Rate: 2.49 Gbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G692, ITU-T G958
- Transmitter
  - Max. Transmitter Output Power: 0 dBm
  - Min. Transmitter Output Power: -2 dBm
  - Center Wavelength: ±.25 nm
  - Transmitter: Electro-absorption laser
- Receiver
  - Max. Receiver Level: -8 dBm
  - Min. Receiver Level: -28 dBm
  - Receiver: InGaAs APD photo detector
  - Link Loss Budget: 26 dB min., with 1 dB dispersion penalty
- Environmental
  - Operating Temperature:

    C-Temp: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 31.20 W, 0.65 amps, 106.53 BTU/Hr.
- Dimensions
  - Height:12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.
  - Card Weight: 2.9 lbs, 1.3 kg
- Compliance
  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
 - Eye Safety Compliance: Class I

4.29 OC192 LR/STM64 LH 1550 Card

The OC192 LR/STM64 LH 1550 card provides one long-range SONET/SDH OC-192 port compliant with the International Telecommunication Union's G.707, G.957, and Telcordia's GR-1377 and GR-253. The card port operates at 9.96 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 VT and non-concatenated or concatenated payloads.

Figure 4-31 shows the OC192 LR/STM64 LH 1550 faceplate and a block diagram of the card. shows an enlarged view of the faceplate warning.

Figure 4-31   OC192 LR/STM64 LH 1550 faceplate and block diagram
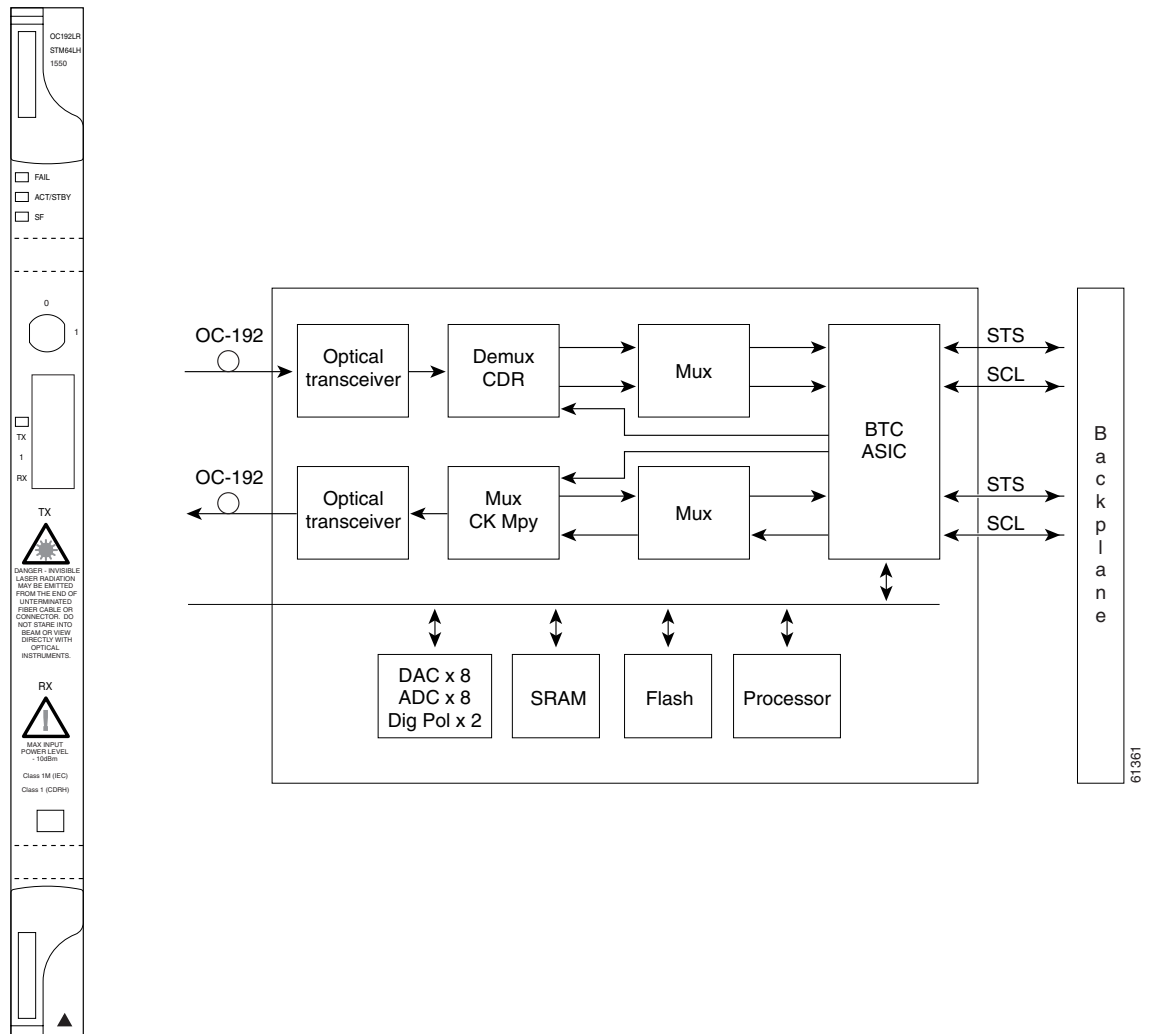
Figure 4-32   Enlarged section of the OC192 LR/STM64 LH 1550 faceplate

TX

DANGER - INVISIBLE
LASER RADIATION
MAY BE EMITTED
FROM THE END OF
UNTERMINATED
FIBER CABLE OR
CONNECTOR. DO
NOT STARE INTO
BEAM OR VIEW
DIRECTLY WITH
OPTICAL
INSTRUMENTS.

RX

MAX INPUT
POWER LEVEL
- 10dBm

Class 1M (IEC)

Class 1 (CDRH)

67465
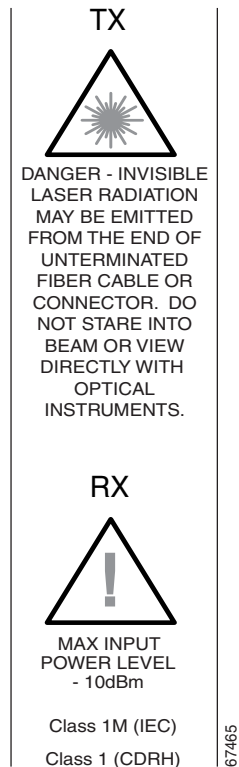
⚠ **Caution**   You must use a 19 to 24 dB (20 recommended) fiber attenuator when connecting a fiber loopback to an OC192 LR/STM64 LH 1550 card. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC-192 card. A Tx to Rx connection that is not attenuated will damage the receiver.

You can install OC192 LR/STM64 LH 1550 cards in any high-speed slot on the ONS 15454 and provision the card as a drop or span card in a two-fiber or four-fiber BLSR, UPSR, or in an ADM (linear) configuration.

The OC-192 card port features a 1550 nm laser and contains a transmit and receive connector (labeled) on the card faceplate.

⚠ **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).**

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 may occur.

The OC192 LR/STM64 LH 1550 card detects SF, LOS, or LOF conditions on the optical facility. See Chapter 1, "Alarm Troubleshooting" for a description of these conditions. The card also counts section and line BIT errors from B1 and B2 byte registers in the section and line overhead.

4.29.1 OC192 LR/STM64 LH 1550 Card-Level Indicators

The OC192 LR/STM64 LH 1550 card has three card-level LED indicators.

Table 4-40   OC192 LR/STM64 LH 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
ACT/STBY LED **Green (Active)** **Amber (Standby)**	When the ACTV/STBY LED is green, the OC-192 card is operational and ready to carry traffic. When the ACTV/STBY LED is amber, the OC-192 card is operational and in standby (protect) mode.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

4.29.2 OC192 LR/STM64 LH 1550 Port-Level Indicators

You can find the status of the OC192 LR/STM64 LH 1550 card port using the LCD screen on the ONS 15454 fan-tray assembly. Use the LCD to view the status of the port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

> **⚠ 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.**

4.29.3 OC192 LR/STM64 LH 1550 Compatibility

Use the XC10G card, the TCC+ card, the new 15454-SA-ANSI shelf assembly, and Software R3.1 or higher to enable the OC192 LR/STM64 LH 1550 card.

4.29.4 OC192 LR/STM64 LH 1550 Card Specifications

- Line
  - Bit Rate: 9.96 Gbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm Single Mode
- Loopback Modes: Terminal and Facility

✎

Note   You must use a 19 to 24 dB (20 recommended) fiber attenuator when connecting a fiber loopback
to an OC192 LR/STM64 LH 1550 card. Never connect a direct fiber loopback.

- – Connectors: SC
- – Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G.707, ITU-T G.957
- Transmitter
  - – Max. Transmitter Output Power: +10 dBm
  - – Min. Transmitter Output Power: +7 dBm
  - – Center Wavelength: 1530 nm – 1565 nm
  - – Nominal Wavelength: 1550 nm
  - – Transmitter: LN (Lithium Niobate) external modulator transmitter
- Receiver
  - – Max. Receiver Level: -10 dBm
  - – Min. Receiver Level: -19 dBm
  - – Receiver: APD/TIA
  - – Link Loss Budget: 24 dB min., with no dispersion or 22 dB optical path loss at BER = 1- exp
    (-12) including dispersion
- Environmental
  - – Operating Temperature:
    C-Temp (15454-OC192LR1550): 0 to +55 degrees Celsius
  - – Operating Humidity: 5 - 95%, non-condensing
  - – Power Consumption: 72.20 W, 1.50 amps, 246.52 BTU/Hr.
- Dimensions
  - – Height:12.650 in.
  - – Width: 0.716 in.
  - – Depth: 9.000 in.
  - – Card Weight: 3.1 lbs, 1.3 kg
- Compliance
  - – ONS 15454 OC192/STM64 cards, when installed in a system, comply with these standards:
    Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
  - – Eye Safety Compliance: Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC
   60825-12001-01) laser products

4.30 E100T-12 Card

Do not use the E100T-12 when the XC10G cross-connect card is in use. The ONS 15454 uses E100T-12
cards for Ethernet (10 Mbps) and Fast Ethernet (100 Mbps). Each card provides 12 switched, IEEE
802.3-compliant, 10/100 Base-T Ethernet ports that can independently detect the speed of an attached

device (auto-sense) and automatically connect at the appropriate speed. The ports auto-configure to operate at either half or full duplex and determine whether to enable or disable flow control. You can also configure Ethernet ports manually. Figure 4-33 shows the faceplate and a block diagram of the card.

Figure 4-33   E100T-12 faceplate and block diagram
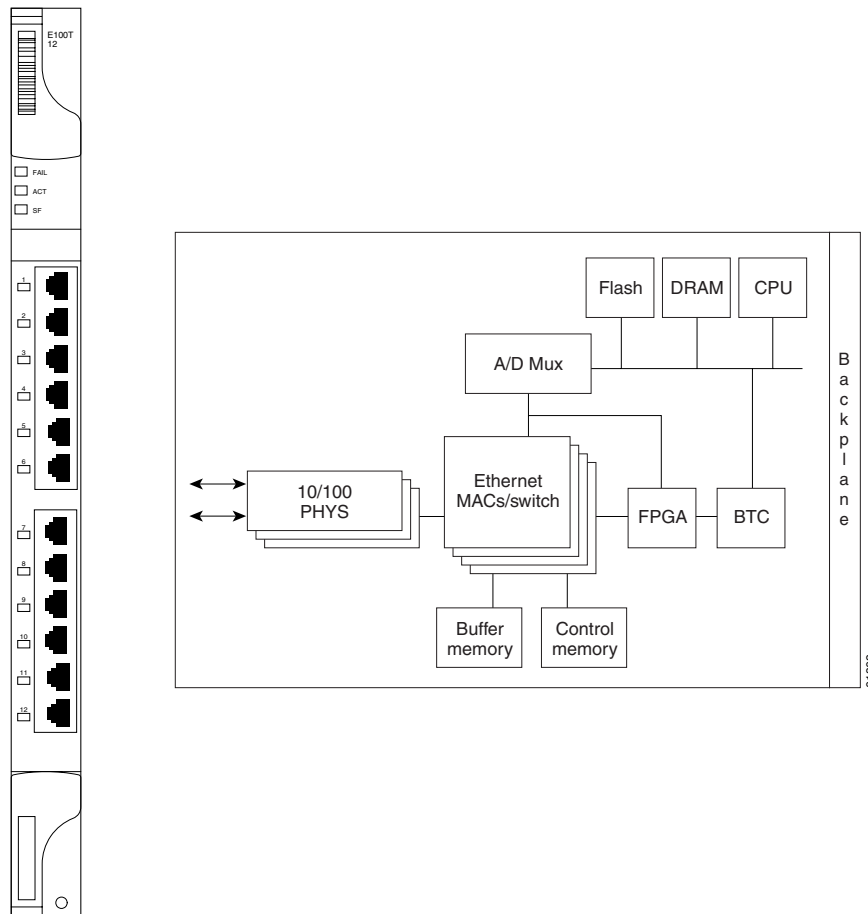
The E100T-12 Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This Ethernet capability enables network operators to provide multiple 10/100 Mbps access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. It enables the efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic.

Each E100T-12 card supports standards-based, wire-speed, layer 2 Ethernet switching between its Ethernet interfaces. The 802.1Q tag logically isolates traffic (typically subscribers). 802.1Q also supports multiple classes of service.

You can install the E100T-12 card in any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 can act independently or as a single Ethernet switch. You can create logical SONET ports by provisioning a number of STS channels to the packet switch entity within the ONS 15454. Logical ports can be created with a bandwidth granularity of STS-1. The ONS 15454 supports STS-1, STS-3c, STS-6c, or STS-12c circuit sizes.

Note   When making an STS-12c Ethernet circuit, the E100 or E1000 cards must be configured as single-card EtherSwitch.

4.30.1 E100T-12 Card-Level Indicators

The E100T-12 card faceplate has two card-level LED indicators.

Table 4-41   E100T-12 Card-Level Indicators

Card-Level Indicators	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-12 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-12. When the ACT LED is green it indicates that the E100T-12 card is active and the software is operational.
SF LED	Not used

4.30.2 E100T-12 Port-Level Indicators

The E100T-12 card also has 12 pairs of LEDs (one pair for each port) to indicate port conditions. You can find the status of the E100T-12 card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

Table 4-42   E100T-12 Port-Level Indicators

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Green Light Off	Inactive Connection or Unidirectional Traffic

4.30.3 E100T-12 Compatibility

Do not use the E100T-12 card with the XC10G card. If you want to use the XC10G card, the E100T-G is compatible with the XC10G.

4.30.4 E100T-12 Card Specifications

- • Environmental
    - – Operating Temperature:

C-Temp (15454-E100T): 0 to +55 degrees Celsius

- – Operating Humidity: 5 - 95%, non-condensing

- – Power Consumption: 65 W, 1.35 amps, 221.93 BTU/Hr.

- • Dimensions

    - – Height: 12.650 in.

    - – Width: 0.716 in.

    - – Depth: 9.000 in.

    - – Card Weight: 2.3 lbs, 1.0 kg

- • Compliance

    - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.31 E100T-G Card

Use the E100T-G when the XC10G cross-connect card is in use. The ONS 15454 uses E100T-G cards for Ethernet (10 Mbps) and Fast Ethernet (100 Mbps). Each card provides 12 switched, IEEE 802.3-compliant, 10/100 Base-T Ethernet ports that can independently detect the speed of an attached device (auto-sense) and automatically connect at the appropriate speed. The ports auto-configure to operate at either half or full duplex and determine whether to enable or disable flow control. You can also configure Ethernet ports manually. Figure 4-34 shows the faceplate and a block diagram of the card.

Figure 4-34   E100T-G faceplate and block diagram
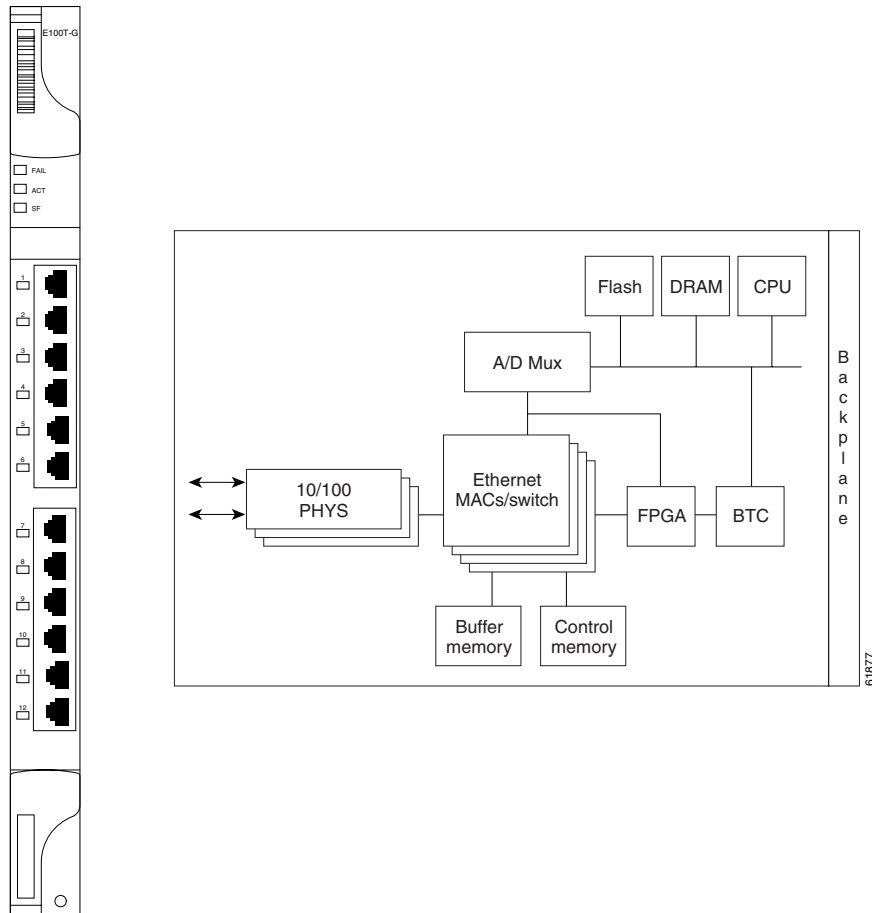
The E100T-G Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This Ethernet capability enables network operators to provide multiple 10/100 Mbps access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. It enables the efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic.

Each E100T-G card supports standards-based, wire-speed, layer 2 Ethernet switching between its Ethernet interfaces. The 802.1Q tag logically isolates traffic (typically subscribers). 802.1Q also supports multiple classes of service.

You can install the E100T-G card in any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 can act independently or as a single Ethernet switch. You can create logical SONET ports by provisioning a number of STS channels to the packet switch entity within the ONS 15454. Logical ports can be created with a bandwidth granularity of STS-1. The ONS 15454 supports STS-1, STS-3c, STS-6c, or STS-12c circuit sizes.

Note   When making an STS-12c Ethernet circuit, the E100 or E1000 cards must be configured as single-card EtherSwitch.

4.31.1 E100T-G Card-Level Indicators

The E100T-G card faceplate has two card-level LED indicators.

Table 4-43   E100T-G Card-Level Indicators

Card-Level Indicators	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

4.31.2 E100T-G Port-Level Indicators

The E100T-G card also has 12 pairs of LEDs (one pair for each port) to indicate port conditions. You can find the status of the E100T-G card port using the LCD screen on the ONS 15454 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. See Chapter 1, "Alarm Troubleshooting" for a complete description of the alarm messages.

Table 4-44   E100T-G Port-Level Indicators

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Green Light Off	Inactive Connection or Unidirectional Traffic

4.31.3 E100T-G Compatibility

Use the E100T-G when the XC10G cross-connect card is in use.

4.31.4 E100T-G Card Specifications

- Environmental
  - Operating Temperature:
    C-Temp (15454-E100T-G): 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 65 W, 1.35 amps, 221.93 BTU/Hr.
- Dimensions
  - Height: 12.650 in, Width: 0.716 in., Depth: 9.000 in.

- Card Weight: 2.3 lbs, 1.0 kg
- Compliance
  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

4.32 E1000-2 Card

Do not use the E1000-2 when the XC10G cross-connect card is in use. The ONS 15454 uses E1000-2 cards for Gigabit Ethernet (1000 Mbps). The E1000-2 card provides two IEEE-compliant, 1000 Mbps ports for high-capacity customer LAN interconnections. Each port supports full-duplex operation. Figure 4-35 shows the card faceplate and a block diagram of the card.

The E1000-2 card uses standard Cisco gigabit interface converter (GBIC) modular receptacles for the optical ports. GBICs are hot-swappable input/output devices that plug into a Gigabit Ethernet port to link the port to the fiber-optic network. Cisco provides two GBIC models: one for short-reach applications and one for long-reach applications. The short-reach model connects to multimode fiber and the long-reach model requires single-mode fiber.

For Software R2.2.0 and later, both GBIC modules are offered as separate orderable products: 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. For more information see the *Cisco ONS 15454 Installation and Operations Guide.*

Figure 4-35   E1000-2 faceplate and block diagram
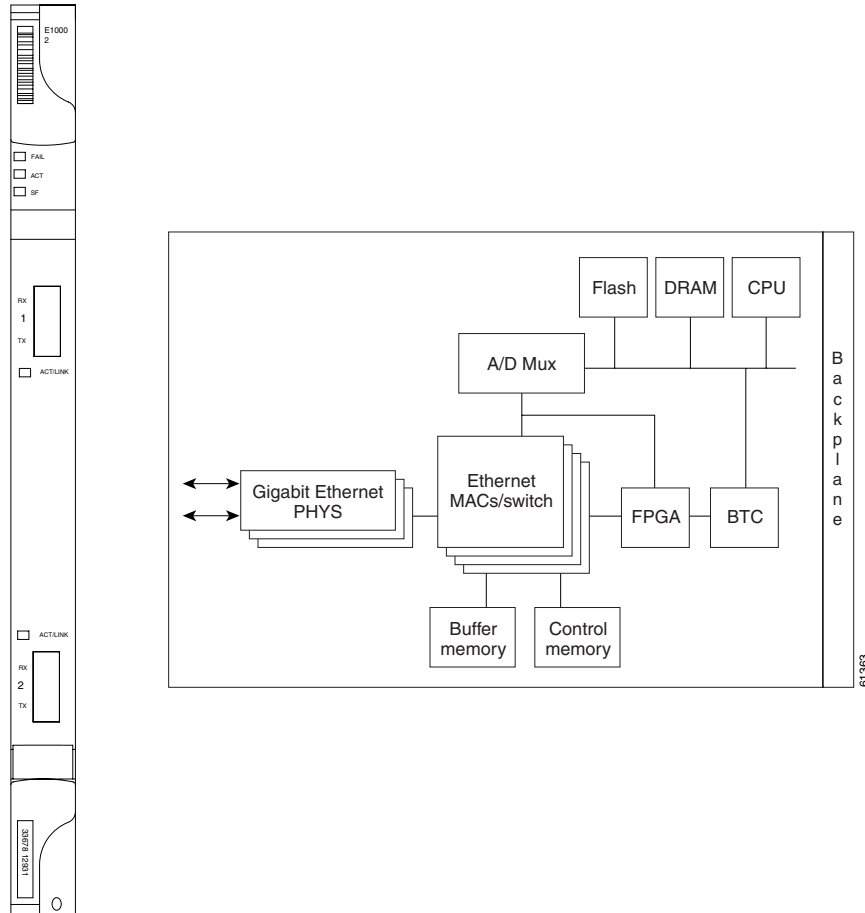
The E1000-2 Gigabit Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This enables network operators to provide multiple 1000 Mbps access drops for high-capacity customer LAN interconnects. It enables efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic.

Each E1000-2 card supports standards-based, layer 2 Ethernet switching between its Ethernet interfaces and SONET interfaces on the ONS 15454. The 802.1Q VLAN tag logically isolates traffic (typically subscribers). The E1000-2 supports two 802.1Q.

You can install the E1000-2 card into any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 can act together as a single switching entity or as an independent single switch supporting a variety of SONET port configurations.

You can create logical SONET ports by provisioning STS channels to the packet switch entity within the ONS 15454. Logical ports can be created with a bandwidth granularity of STS-1. The ONS 15454 supports STS-1, STS-3c, STS-6c, or STS-12c circuit sizes.

Note When making an STS-12c Ethernet circuit, the E100 or E1000 cards must be configured as single-card EtherSwitch.

4.32.1 E1000-2 Card-Level Indicators

The E1000-2 card faceplate has two card-level LED indicators.

Table 4-45   E1000-2 Card-Level Indicators

Card-Level Indicators	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 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. When the ACT LED is green it indicates that the E1000-2 card is active and the software is operational.
SF LED	Not used

4.32.2 E1000-2 Port-Level Indicators

The E1000-2 card also has one bicolor LED per port. When the green LINK LED is on, carrier 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, or the card is carrying unidirectional traffic. The amber port ACT LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.

Table 4-46   E1000-2 Port-Level Indicators

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Green Light Off	Inactive Connection or Unidirectional Traffic

4.32.3 E1000-2 Compatibility

Do not use the E1000-2 card with the XC10G card. If you want to use the XC10G card, the E1000-2-G is compatible with the XC10G.

4.32.4 E1000-2 Card Specifications

- Environmental
  - Operating Temperature:
    C-Temp (15454-E1000-2): 0 to +55 degrees Celsius
  - Operating Humidity: 5- 95%, non-condensing
  - Power Consumption: 53.50 W, 1.11 amps, 182.67 BTU/Hr.
- Dimensions
  - Height: 12.650 in.

- – Width: 0.716 in.

- – Depth: 9.000 in.

- – Card Weight: 2.1 lbs, 0.9 kg

- • Compliance

  - – ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  - – Eye Safety Compliance: Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products

4.33 E1000-2-G Card

Use the E1000-2-G when the XC10G cross-connect card is in use. The ONS 15454 uses E1000-2-G cards for Gigabit Ethernet (1000 Mbps). The E1000-2-G card provides two IEEE-compliant, 1000 Mbps ports for high-capacity customer LAN interconnections. Each port supports full-duplex operation. Figure 4-36 shows the card faceplate and a block diagram of the card.

The E1000-2-G card uses standard Cisco gigabit interface converter (GBIC) modular receptacles for the optical ports. GBICs are hot-swappable input/output devices that plug into a Gigabit Ethernet port to link the port to the fiber-optic network. Cisco provides two GBIC models: one for short-reach applications and one for long-reach applications. The short-reach model connects to multimode fiber and the long-reach model requires single-mode fiber.

For Software R2.2.0 and later, both GBIC modules are offered as separate orderable products: 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. For more information see the *Cisco ONS 15454 Installation and Operations Guide*.

Figure 4-36   E1000-2-G faceplate and block diagram
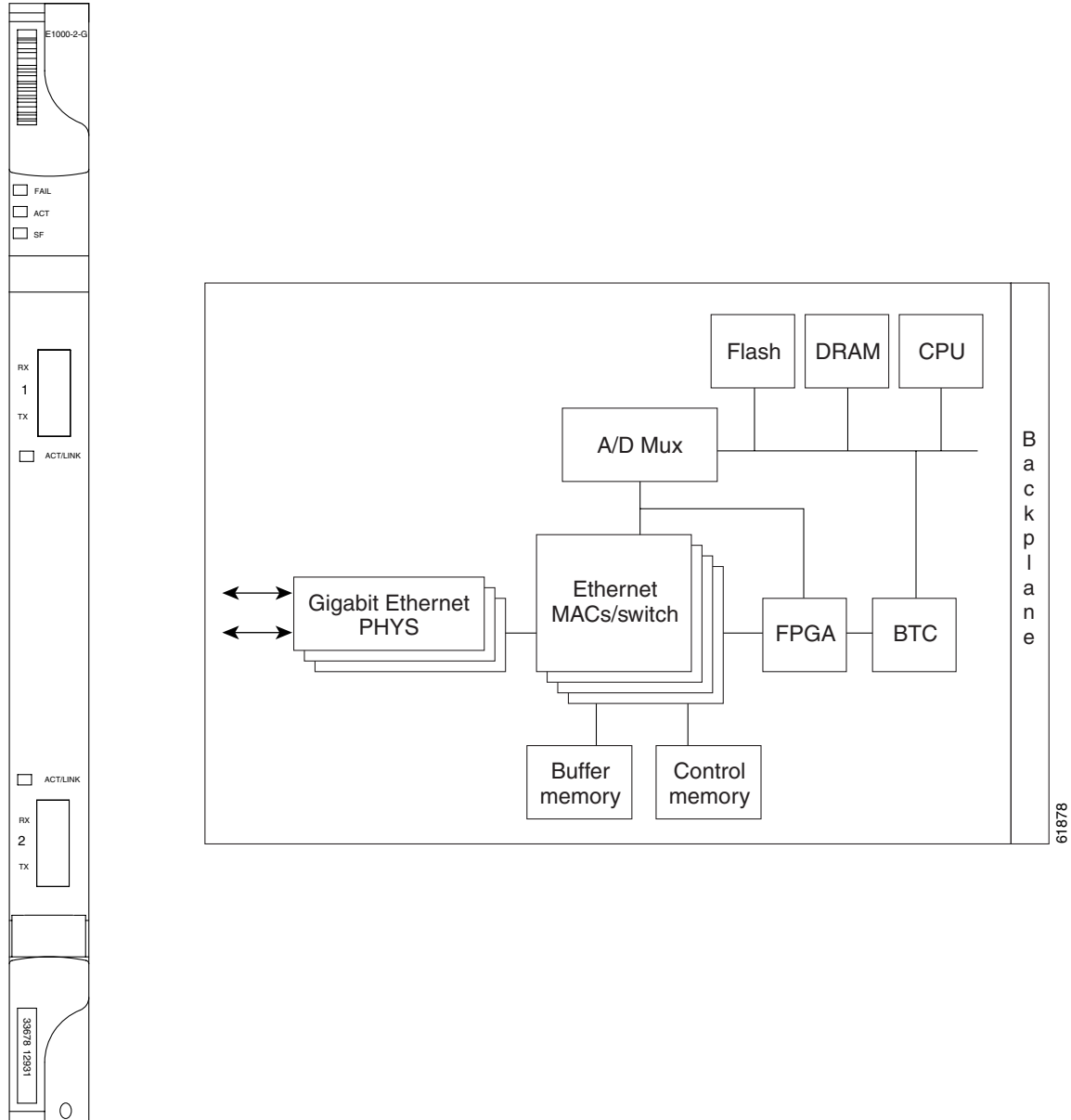
The E1000-2-G Gigabit Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This enables network operators to provide multiple 1000 Mbps access drops for high-capacity customer LAN interconnects. It enables efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic.

Each E1000-2-G card supports standards-based, layer 2 Ethernet switching between its Ethernet interfaces and SONET interfaces on the ONS 15454. The 802.1Q VLAN tag logically isolates traffic (typically subscribers). The E1000-2-G supports two 802.1Q.

You can install the E1000-2-G card into any multispeed slot. Multiple Ethernet cards installed in an ONS 15454 can act together as a single switching entity or as an independent single switch supporting a variety of SONET port configurations.

You can create logical SONET ports by provisioning STS channels to the packet switch entity within the ONS 15454. Logical ports can be created with a bandwidth granularity of STS-1. The ONS 15454 supports STS-1, STS-3c, STS-6c, or STS-12c circuit sizes.

Note   When making an STS-12c Ethernet circuit, the E100 or E1000 cards must be configured as a Single-card EtherSwitch.

4.33.1 E1000-2-G Card-Level Indicators

The E1000-2-G card faceplate has two card-level LED indicators.

Table 4-47   E1000-2-G Card-Level Indicators

Card-Level Indicators	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

4.33.2 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, carrier 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, or the card is carrying unidirectional traffic. The amber port ACT LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.

Table 4-48   E1000-2-G Port-Level Indicators

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Green Light Off	Inactive Connection or Unidirectional Traffic

4.33.3 E1000-2-G Compatibility

Use the E1000-2-G when the XC10G cross-connect card is in use.

4.33.4 E1000-2-G Card Specifications

- Environmental

Cisco ONS 15454 Troubleshooting and Maintenance Guide, R3.2

- Operating Temperature:

  C-Temp (15454-E1000-2-G): 0 to +55 degrees Celsius

- Operating Humidity: 5- 95%, non-condensing

- Power Consumption: 53.50 W, 1.11 amps, 182.67 BTU/Hr.

- Dimensions

  - Height: 12.650 in.

  - Width: 0.716 in.

  - Depth: 9.000 in.

  - Card Weight: 2.1 lbs, 0.9 kg

- Compliance

  - ONS 15454 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950

  - Eye Safety Compliance: Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products

4.34 G1000-4 Card

Use the G1000-4 card when the XC10G card is in use. The ONS 15454 uses G1000-4 cards for Gigabit Ethernet (1000 Mbps). The G1000-4 card provides four ports of IEEE-compliant, 1000 Mbps interfaces. Each port supports full-duplex operation for a maximum bandwidth of OC-48 on each card. The G1000-4 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;

- 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 ten kilometers. Figure 4-37 shows the card faceplate and the block diagram of the card.

Figure 4-37   G1000-4 faceplate and block diagram
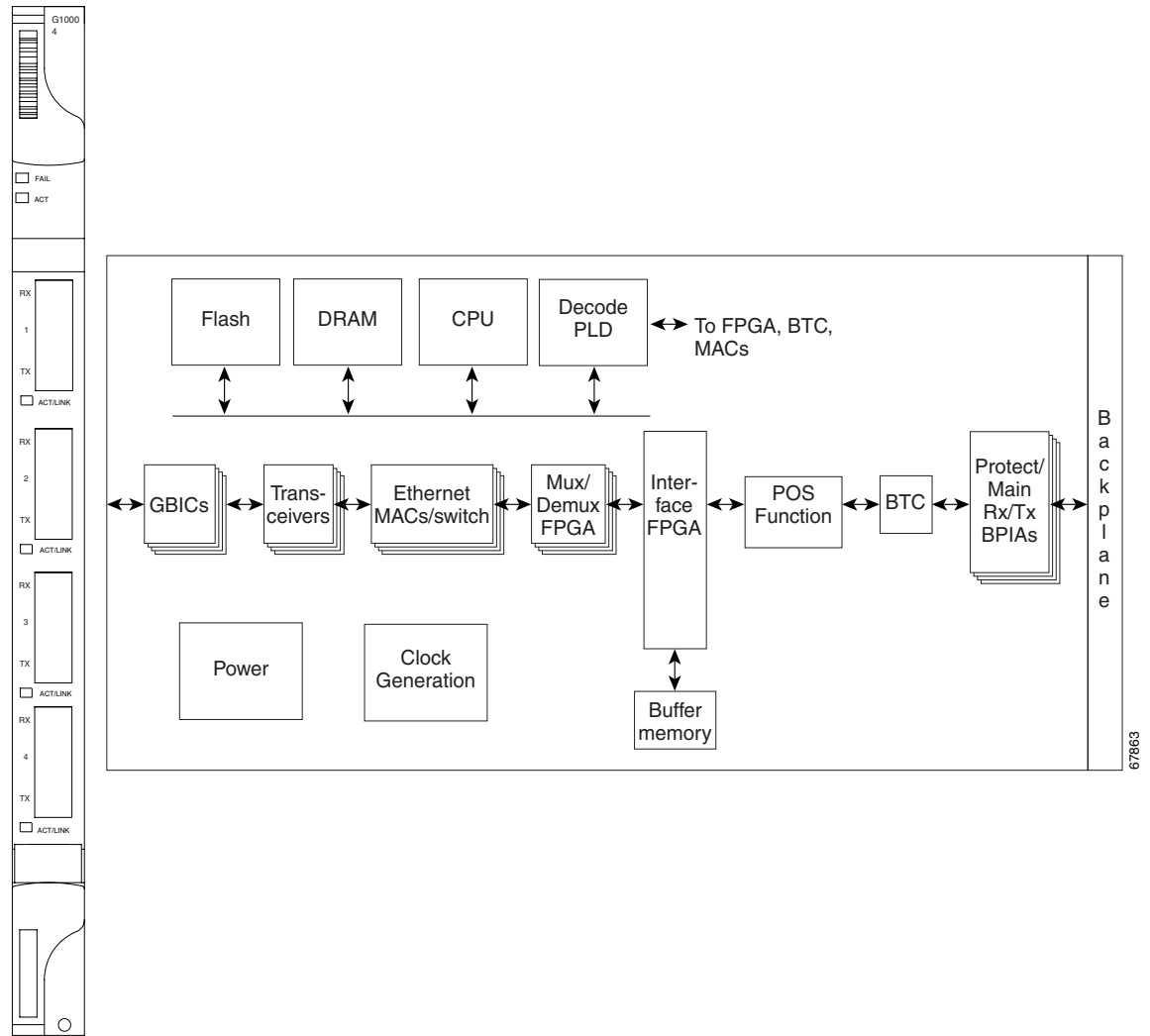
The G1000-4 Gigabit Ethernet card provides high-throughput, low latency transport of Ethernet encapsulated traffic (IP and other layer 2 or layer 3 protocols) across a SONET network. Carrier-class Ethernet transport is achieved by hitless (< 50 msec) performance in the event of any failures or protection switches (such as 1+1 APS, UPSR, or BLSR). Full provisioning support is possible via CTC, TL1, or CTM.

You can install the G1000-4 card into any multispeed slot for a total shelf capacity of 48 Gigabit Ethernet ports.

Note   The practical G1000-4 port per shelf limit is 40, because at least 2 slots are typically filled by OC-N cards such as the OC-192.

The circuit sizes supported are STS-1, STS-3c, STS-6c, STS-9c, STS-24c, STS-48c.

4.34.1 G1000-4 Card-Level Indicators

The G1000-4 card faceplate has two card-level LED indicators.

Table 4-49   G1000-4 Card-Level Indicators

Card-Level LEDs	Description
FAIL LED (red)	The red FAIL LED indicates 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 turns 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.

4.34.2 G1000-4 Port-Level Indicators

The G1000-4 card also has one bicolor LED per port. The following table describes the status that each color represents.

Table 4-50   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 set-up, an error on line or a non-enabled port may 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.

4.34.3 G1000-4 Compatibility

Use the G1000-4 when the XC10G cross-connect card is in use.

4.34.4 G1000-4 Card Specifications

- Environmental
    - Operating Temperature:
      C-Temp (15454-G1000-4): 0 to +55 degrees Celsius
    - Operating Humidity: 5- 95%, non-condensing
    - Power Consumption: 63.00 W, 1.31 amps, 215.11 BTU/Hr.
- Dimensions
    - Height: 12.650 in.

- – Width: 0.716 in.
- – Depth: 9.000 in.
- – Card Weight: 2.1 lbs, 0.9 kg

ACRONYMS
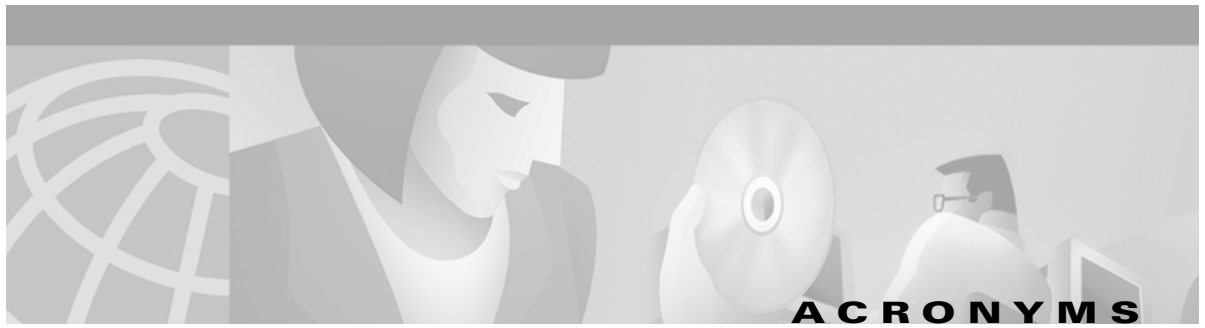
Numerics

10BaseT

standard 10 megabit per second local area network over unshielded twisted pair copper wire

100BaseT

standard 100 megabit per second ethernet network

100BaseTX

specification of 100BaseT that supports full duplex operation

A

ACO

Alarm Cutoff

ACT/STBY

Active/Standby

ADM

Add-Drop Multiplexer

AIC

Alarm Interface Controller

AID

Access Identifier

AIP

Alarm Interface Panel

AIS

Alarm Indication Signal

AIS-L

Line Alarm Indication Signal

AMI

Alternate Mark Inversion

ANSI

American National Standards Institute

APS

Automatic Protection Switching

ARP

Address Resolution Protocol

ATAG

Autonomous Message Tag

ATM

Asynchronous Transfer Mode

AWG

American Wire Gauge

B

B8ZS

Bipolar 8 Zero Substitution

BER

Bit Error Rate

BIC

Backplane Interface Connector

BIP

Bit Interleaved Parity

BITS

Building Integrated Timing Supply

BLSR

Bidirectional line switched ring

BNC

Bayonet Neill-Concelman (coaxial cable bayonet locking connector)

BPDU

Bridge Protocol Data Unit

C

CAT 5

Category 5 (cabling)

CCITT

Consultative Committee International Telegraph and Telephone (France)

CEO

Central Office Environment

CEV

Controlled Environment Vaults

CLEI

Common Language Equipment Identifier code

CLNP

Correctionless Network Protocol

CMIP

Common Management Information Protocol

cm

centimeter

COE

Central Office Environment

CORBA

Common Object Request Broker Architecture

CPE

Customer Premise Environments

CTAG

Correlation Tag

CTC

Cisco Transport Controller

D

DCC

Data Communications Channel

DCN

Data Communications Network

DCS

Distributed Communications System

DRAM

Dynamic Random Access Memory

DS-1

Digital Signal Level One

DS-3

Digital Signal Level Three

DS1-14

Digital Signal Level One (14 ports)

DS1N-14

Digital Signal Level One (N-14 ports)

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

E

EDFA

Erbium Doped Fiber Amplifier

EFT

Electrical Fast Transient/Burst

EIA

Electrical Interface Assemblies

ELR

Extended Long Reach

EMI

Electromagnetic interface

EML

Element Management Layer

EMS

Element Management System

EOW

Express Orderwire

ERDI

Enhanced Remote Defect Indicator

ES

Errored Seconds

ESD

Electrostatic Discharge

ESF

Extended Super Frame

ETSI

European Telecommunications Standards Institute

F

FC

Failure Count

FDDI

Fiber Distributed Data Interface

FE

Frame Bit Errors

FG1

Frame Ground #1(pins are labeled "FG1," "FG2," etc.)

FSB

Field Service Bulletin

G

Gbps

Gigabits per second

GBIC

Gigabit Interface Converter

GR-253-CORE

General Requirements #253 Council Of Registrars

GR-1089

General Requirements #1089

GUI

Graphical User Interface

H

HDLC

High-Level Data Link Control

I

IEC

InterExchange Carrier

IEEE

Institute of Electrical and Electronics Engineers

IETF

Internet Engineering Task Force

IP

Internet Protocol

IPPM

Intermediate-Path Performance Monitoring

I/O

Input/Output

ITU-T

The International Telecommunication Union-Telecommunication Standards Sector

J

JRE

Java Runtime Environment

L

LAN

Local Area Network

LCD

Liquid Crystal Display

LDCC

Line Data Communications Channel

LOP

Loss of Pointer

LOS

Loss of Signal

LOF

Loss of Frame

LOW

Local Orderwire

LTE

Line Terminating Equipment

LVDS

Low Voltage Differential Signal

M

MAC

Media Access Control

Mbps

Million bits per second, or Million bytes per second

Mhz

Megahertz

MIB

Management Information Bases

MIME

Multipurpose Internet Mail Extensions

Mux/Demux

Multiplexer/Demultiplexer

N

NE

Network Element

NEL

Network Element Layer

NEBS

Network Equipment-Building Systems

NML

Network Management Layer

NMS

Network Management System

O

OAM&P

Operations, Administration, Maintenance, and Provisioning

OC

Optical carrier

OOS AS

Out of Service Assigned

OSI

Open Systems Interconnection

OSPF

Open Shortest Path First

OSS

Operations Support System

OSS/NMS

Operations Support System/Network Management System

P

PCM

Pulse Code Modulation

PCMCIA

Personal Computer Memory Card International Association

PCN

Product Change Notices

PDI-P

STS Payload Defect Indication-Path

POP

Point of Presence

PM

Performance Monitoring

PPMN

Path-Protected Mesh Network

PSC

Protection Switching Count

PSD

Protection Switching Duration

PTE

Path Terminating Equipment

R

RAM

Random Access Memory

RDI-L

Remote Defect Indication Line

RES

Reserved

RJ45

Registered Jack #45 (8 pin)

RMA

Return Material Authorization

RMON

Remote Network Monitoring

RS232

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication

Rx

Receive

S

SCI

Serial Communication Interface

SCL

System Communications Link

SDCC

Section Data Communications Channel

SDH/SONET

Synchronous Digital Hierarchy/Synchronous Optical Network

SEF

Severely Errored Frame

SELV

Safety Extra Low Voltage

SES

Severely Errored Seconds

SF

Super Frame

SML

Service Management Layer

SMF

Single Mode Fiber

SNMP

Simple Network Management Protocol

SNTP

Simple Network Time Protocol

SONET

Synchronous Optical Network

SPE

Synchronous Payload Envelope

SSM

Synchronous Status Messaging

STA

Spanning Tree Algorithm

STP

Shielded Twisted Pair

STS-1

Synchronous Transport Signal Level 1

SWS

SONET WAN Switch

SXC

SONET Cross Connect ASIC

T

TAC

Technical Assistance Center

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

TDS

Time Division Switching

TID

Target Identifier

TL1

Transaction Language 1

TLS

Transparent LAN service

TMN

Telecommunications Management Network

TSA

Time Slot Assignment

TSI

Time-Slot Interchange

Tx

Transmit

U

UAS

Unavailable Seconds

UDP/IP

User Datagram Protocol/Internet Protocol

UID

User Identifier

UPSR

Unidirectional Path Switched Ring

UTC

Universal Time Coordinated

UTP

Unshielded Twisted Pair

V

VDC

Volts Direct Current

VLAN

Virtual Local Area Network

VPN

Virtual Private Network

VT1.5

Virtual Tributary equals 1.544 megabits per second

W

WAN

Wide Area Network

W

Watts

X

XC

Cross-Connect

XCVT

Cross-Connect Virtual Tributary

X.25

Protocol providing devices with direct connection to a packet switched network

GLOSSARY

Numerics

1:1 protection

A card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot. 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 back to the working card if this option is set. This protection scheme is specific to electrical cards.

1+1 protection

A card protection scheme that pairs a single working card with a single dedicated protect card. A term specific to optical cards.

1:N protection

A card protection scheme that allows a single card to protect several working cards. When the failure on the working card is resolved, traffic reverts back to the working card. A term specific to electrical cards.

A

Access drop

Points where network devices can access the network.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the part that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

Add/drop multiplexer. ADM allows a signal to be added into or dropped from a SONET span.

Agent
1. Generally, software that processes queries and returns replies on behalf of an application.
2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

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.

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.

APS

Automatic Protection Switching. SONET switching mechanism that routes traffic from working lines to protect lines in case a line card failure or fiber cut occurs.

ATAG

Autonomous Message Tag. ATAG is used for TL1 message sequencing.

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.

BER

Bit Error Rate. Ratio of received bits that contain errors.

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.

Blue band

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

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.

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.

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.

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.

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.

CTC

Cisco Transport Controller. A Java-based graphical user interface (GUI) that allows operations, administration, maintenenance, 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 equipment.

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 section DCC (SDCC) or line overhead (LDCC.)

Demultiplex

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. See also *Multiplexing*.

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.

EIA

Electrical Interface Assemblies. Provides connection points for the ONS 15454 and DS-1, DS-3, or EC-1 units.

EMI

Electromagnetic Interference. Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

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

Express Orderwire. A permanently connected voice circuit between selected stations for technical control purposes.

Ethernet switch

An Ethernet data switch. Ethernet switches provide the capability to increase the 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.

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*.

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.

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.

Free run synchronization mode

Occurs when the external timing sources have been disabled and the ONS 15454 is receiving timing from its Stratum 3 level internal timing source.

G

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.

H

Hard reset

The physical removal and insertion of a card. 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

Input alarms

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

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.

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.

K

K bytes

Automatic protection switching bytes. K bytes are 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.

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 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 is intact.

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.

LOW

Local Orderwire. A communications circuit between a technical control center and selected terminal or repeater locations.

M

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.

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.

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 logical signals to be transmitted simultaneously across a single physical channel. Compare with *Demultiplex.*

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.

Network number

Part of an IP address that specifies the network where the host belongs.

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.

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.

Output contacts (alarms)

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).

Ping

Packet internet grouper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

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.

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.*

Q

Queue

In routing, a backlog of packets waiting to be forwarded over a router interface.

R

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 operate on wavelengths between 1547.72nm and 1560.61nm.

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 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.

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.

S

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 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.

Spanning tree

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

Sync 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*.

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

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, STA,* and *Learning bridge.*

STS-1

Synchronous Transport Signal 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.*

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*.

Tag

Identification information, including a number plus other information.

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.

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.

TLS

Transparent LAN Service. Provides private network service across a SONET backbone.

Transponder

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength.

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.

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*.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. See also *encapsulation*.

U

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.

Upstream

Set of frequencies used to send data from a subscriber to the headend.

V

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.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

P

R