

Cisco ONS 15454 Troubleshooting Guide

Product and Documentation Release 3.4
Last Updated: December 30, 2004

Corporate Headquarters

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

Customer Order Number: DOC-7814869=
Text Part Number: 78-14869-01



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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0501R)



About this Manual	xxiii
Obtaining Documentation	xxiii
World Wide Web	xxiii
Documentation CD-ROM	xxiii
Ordering Documentation	xxiii
Documentation Feedback	xxiv
Obtaining Technical Assistance	xxiv
Cisco.com	xxiv
Technical Assistance Center	xxv
Cisco TAC Web Site	xxv
Cisco TAC Escalation Center	xxv

CHAPTER 1

General Troubleshooting	1-1
1.1 Network Troubleshooting Tests	1-2
1.2 Identify Points of Failure on a DS-N Circuit Path	1-4
1.2.1 Perform a Facility Loopback on a Source DS-N Port	1-4
Create the Facility Loopback on the Source DS-N port	1-4
Test the Facility Loopback Circuit	1-5
Test the DS-N Cabling	1-6
Test the DS-N Card	1-6
Test the EIA	1-7
1.2.2 Perform a Hairpin on a Source Node Port	1-8
Create the Hairpin on the Source Node Port	1-8
Test the Hairpin Circuit	1-9
Test the Standby Cross-Connect Card	1-9
Retest the Original Cross-Connect Card	1-10
1.2.3 Perform a Terminal Loopback on a Destination DS-N Port	1-11
Create the Terminal Loopback on a Destination DS-N Port	1-11
Test the Terminal Loopback Circuit on the Destination DS-N Port	1-12
Test the Destination DS-N Card	1-13
1.2.4 Perform a Hairpin on a Destination Node	1-14
Create the Hairpin on the Destination Node	1-14
Test the Hairpin Circuit	1-15
Test the Standby Cross-Connect Card	1-15
Retest the Original Cross-Connect Card	1-16

- 1.2.5 Perform a Facility Loopback on a Destination DS-N Port **1-17**
 - Create a Facility Loopback Circuit on a Destination DS-N Port **1-17**
 - Test the Facility Loopback Circuit **1-18**
 - Test the DS-N Cabling **1-18**
 - Test the DS-N Card **1-19**
 - Test the EIA **1-20**
- 1.3 Using the DS3XM-6 Card FEAC (Loopback) Functions **1-21**
 - 1.3.1 FEAC Send Code **1-22**
 - 1.3.2 FEAC Inhibit Loopback **1-22**
 - 1.3.3 FEAC Alarms **1-22**
- 1.4 Identify Points of Failure on an OC-N Circuit Path **1-22**
 - 1.4.1 Perform a Facility Loopback on a Source-Node OC-N Port **1-23**
 - Create the Facility Loopback on the Source OC-N Port **1-23**
 - Test the Facility Loopback Circuit **1-24**
 - Test the OC-N Card **1-24**
 - 1.4.2 Perform a Terminal Loopback on a Source-Node OC-N Port **1-25**
 - Create the Terminal Loopback on a Source Node OC-N Port **1-25**
 - Test the Terminal Loopback Circuit **1-26**
 - Test the OC-N card **1-27**
 - 1.4.3 Perform a Facility Loopback on an Intermediate-Node OC-N Port **1-28**
 - Create the Facility Loopback on an Intermediate-Node OC-N Port **1-28**
 - Test the Facility Loopback Circuit **1-29**
 - Test the OC-N Card **1-30**
 - 1.4.4 Perform a Terminal Loopback on an Intermediate-Node OC-N Port **1-31**
 - Create the Terminal Loopback on an Intermediate-Node OC-N Port **1-31**
 - Test the Terminal Loopback Circuit **1-32**
 - Test the OC-N card **1-33**
 - 1.4.5 Perform a Facility Loopback on a Destination-Node OC-N Port **1-33**
 - Create the Facility Loopback on a Destination-Node OC-N Port **1-34**
 - Test the Facility Loopback Circuit **1-35**
 - Test the OC-N Card **1-35**
 - 1.4.6 Perform a Terminal Loopback on a Destination-Node OC-N Port **1-36**
 - Create the Terminal Loopback on a Destination-Node OC-N Port **1-37**
 - Test the Terminal Loopback Circuit **1-38**
 - Test the OC-N Card **1-38**
- 1.5 Restoring the Database and Default Settings **1-39**
 - 1.5.1 Restore the Node Database **1-39**
 - Restore the Database **1-40**
 - 1.5.2 Restore the Node to Factory Configuration **1-41**

	DLP-244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)	1-42
	DLP-245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)	1-43
1.6	PC Connectivity Troubleshooting	1-45
1.6.1	Unable to Verify the IP Configuration of your PC	1-45
	Verify the IP Configuration of your PC	1-45
1.6.2	Browser Login Does Not Launch Java	1-46
	Reconfigure the PC Operating System Java Plug-in Control Panel	1-46
	Reconfigure the Browser	1-47
1.6.3	Unable to Verify the NIC Connection on your PC	1-47
1.6.4	Verify PC Connection to the ONS 15454 (ping)	1-48
	Ping the ONS 15454	1-48
1.7	CTC Operation Troubleshooting	1-49
1.7.1	Unable to Change Node View to Network View	1-49
	Reset the CTC_HEAP Environment Variable for Windows	1-49
	Reset the CTC_HEAP Environment Variable for Solaris	1-50
1.7.2	Browser Stalls When Downloading CTC JAR Files From TCC+	1-50
	Disable the VirusScan Download Scan	1-50
1.7.3	CTC Does Not Launch	1-51
	Redirect the Netscape Cache to a Valid Directory	1-51
1.7.4	Sluggish CTC Operation or Login Problems	1-51
	Delete the CTC Cache File Automatically	1-52
	Delete the CTC Cache File Manually	1-53
1.7.5	Node Icon is Grey on CTC Network View	1-53
1.7.6	CTC Cannot Launch Due to Applet Security Restrictions	1-53
	Manually Edit the java.policy File	1-54
1.7.7	Java Runtime Environment Incompatible	1-54
	Launch CTC to Correct the Core Version Build	1-55
1.7.8	Different CTC Releases Do Not Recognize Each Other	1-56
	Launch CTC to Correct the Core Version Build	1-56
1.7.9	Username or Password Do Not Match	1-56
	Verify Correct Username and Password	1-57
1.7.10	No IP Connectivity Exists Between Nodes	1-57
1.7.11	DCC Connection Lost	1-57
1.7.12	"Path in Use" Error When Creating a Circuit	1-58
1.7.13	Calculate and Design IP Subnets	1-58
1.7.14	Ethernet Connections	1-59
	Verify Ethernet Connections	1-59
1.7.15	VLAN Cannot Connect to Network Device from Untag Port	1-60
	Change VLAN Port Tag and Untagged Settings	1-61

- 1.7.16 Cross-Connect Card Oscillator Fails 1-62
 - Resolve the XC Oscillator Failure When Slot 8 XC Card is Active 1-63
 - Resolve the XC Oscillator Failure When Slot 10 XC Card is Active 1-63
- 1.8 Circuits and Timing 1-64
 - 1.8.1 Circuit Transitions to Partial State 1-64
 - View the State of Circuit Nodes 1-65
 - 1.8.2 AIS-V on DS3XM-6 Unused VT Circuits 1-65
 - Clear AIS-V on DS3XM-6 Unused VT Circuits 1-66
 - 1.8.3 Circuit Creation Error with VT1.5 Circuit 1-66
 - 1.8.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card 1-67
 - 1.8.5 DS3 Card Does Not Report AIS-P From External Equipment 1-67
 - 1.8.6 OC-3 and DCC Limitations 1-68
 - 1.8.7 ONS 15454 Switches Timing Reference 1-68
 - 1.8.8 Holdover Synchronization Alarm 1-69
 - 1.8.9 Free-Running Synchronization Mode 1-69
 - 1.8.10 Daisy-Chained BITS Not Functioning 1-69
 - 1.8.11 Blinking STAT LED after Installing a Card 1-70
- 1.9 Fiber and Cabling 1-70
 - 1.9.1 Bit Errors Appear for a Traffic Card 1-70
 - 1.9.2 Faulty Fiber-Optic Connections 1-71
 - Verify Fiber-Optic Connections 1-71
 - Replace Faulty Gigabit Interface Converters 1-73
 - Crimp Replacement LAN Cables 1-75
 - 1.9.3 Optical Card Transmit and Receive Levels 1-77
- 1.10 Power and LED Tests 1-78
 - 1.10.1 Power Supply Problems 1-78
 - Isolate the Cause of Power Supply Problems 1-79
 - 1.10.2 Power Consumption for Node and Cards 1-79
 - 1.10.3 Lamp Test for Card LEDs 1-80
 - Verify Card LED Operation 1-80

CHAPTER 2

Alarm Troubleshooting 2-1

- 2.1 Alarm Index by Default Severity 2-1
 - 2.1.1 Critical Alarms (CR) 2-1
 - 2.1.2 Major Alarms (MJ) 2-2
 - 2.1.3 Minor Alarms (MN) 2-2
 - 2.1.4 Conditions (NA or NR) 2-3
- 2.2 Alarm Index By Alphabetical Entry 2-4
- 2.3 Alarm Index by Alarm Type 2-6

2.3.1 Alarm Type/Object Definition	2-13
2.4 Trouble Notifications	2-14
2.4.1 Conditions	2-14
2.4.2 Severities	2-14
2.5 Safety Summary	2-15
2.6 Alarm Procedures	2-15
2.6.1 AIS	2-16
Clear the AIS Condition	2-16
2.6.2 AIS-L	2-16
Clear the AIS-L Condition	2-16
2.6.3 AIS-P	2-16
Clear the AIS-P Condition	2-17
2.6.4 AIS-V	2-17
Clear the AIS-V Condition	2-18
2.6.5 APSB	2-18
Clear the APSB Alarm	2-18
2.6.6 APSCDFLTK	2-18
Clear the APSCDFLTK Alarm	2-19
2.6.7 APSC-IMP	2-19
Clear the APSC-IMP Alarm	2-19
2.6.8 APSCINCON	2-20
Clear the APSCINCON Alarm	2-20
2.6.9 APSCM	2-20
Clear the APSCM Alarm	2-21
2.6.10 APSCNMIS	2-21
Clear the APSCNMIS Alarm	2-21
2.6.11 APSMM	2-22
Clear the APSMM Alarm	2-22
2.6.12 AS-CMD	2-22
Clear the AS-CMD Condition	2-23
2.6.13 AS-MT	2-23
2.6.14 AUTOLSROFF	2-24
Clear the AUTOLSROFF Alarm	2-24
2.6.15 AUTORESET	2-25
Clear the AUTORESET Alarm	2-25
2.6.16 AUTOSW-AIS	2-25
2.6.17 AUTOSW-LOP (STSMON)	2-25
2.6.18 AUTOSW-LOP (VT-MON)	2-26
2.6.19 AUTOSW-PDI	2-26

2.6.20	AUTOSW-SDBER	2-26
2.6.21	AUTOSW-SFBER	2-26
2.6.22	AUTOSW-UNEQ (STSMON)	2-27
2.6.23	AUTOSW-UNEQ (VT-MON)	2-27
2.6.24	BKUPMEMP	2-27
	Clear the BKUPMEMP Alarm	2-27
2.6.25	BLSROSYNC	2-28
	Clear the BLSROSYNC Alarm	2-28
2.6.26	CARLOSS (EQPT)	2-28
	Clear the CARLOSS Alarm	2-28
2.6.27	CARLOSS (E-Series)	2-29
	Clear the CARLOSS Alarm	2-29
2.6.28	CARLOSS (G1000-4)	2-31
	Clear the CARLOSS Alarm	2-31
2.6.29	CLDRESTART	2-33
	Clear the CLDRESTART Condition	2-33
2.6.30	COMIOXC	2-34
	Clear the COMIOXC Condition	2-34
2.6.31	CONCAT	2-35
	Clear the CONCAT Alarm	2-35
2.6.32	CONTBUS-A-18	2-35
	Clear the CONTBUS-A-18 Alarm	2-36
2.6.33	CONTBUS-B-18	2-36
	Clear the CONTBUS-B-18 Alarm	2-36
2.6.34	CONTBUS-IO-A	2-37
	Clear the CONTBUS-IO-A Alarm	2-37
2.6.35	CONTBUS-IO-B	2-38
	Clear the CONTBUS-IO-B Alarm	2-38
2.6.36	CTNEQPT-PBPROT	2-39
	Clear the CTNEQPT-PBPROT Alarm	2-39
2.6.37	CTNEQPT-PBWORK	2-40
	Clear the CTNEQPT-PBWORK Alarm	2-41
2.6.38	DATAFLT	2-42
2.6.39	DS3-MISM	2-42
	Clear the DS3-MISM Condition	2-42
2.6.40	EHIBATVG-A	2-43
2.6.41	EHIBATVG-B	2-43
2.6.42	ELWBATVG-A	2-43
2.6.43	ELWBATVG-B	2-44
2.6.44	EOC	2-44

Clear the EOC Alarm	2-44
2.6.45 EQPT	2-46
Clear the EQPT Alarm	2-46
2.6.46 EQPT-MISS	2-47
Clear the EQPT-MISS Alarm	2-47
2.6.47 E-W-MISMATCH	2-47
Clear the E-W-MISMATCH Alarm in CTC	2-47
Clear the E-W-MISMATCH Alarm with a Physical Switch	2-48
2.6.48 EXCCOL	2-49
Clear the EXCCOL Alarm	2-49
2.6.49 EXERCISE-RING-REQ	2-49
2.6.50 EXERCISE-SPAN-REQ	2-50
2.6.51 EXT	2-50
Clear the EXT Alarm	2-50
2.6.52 EXTRA-TRAF-PREEMPT	2-50
Clear the EXTRA-TRAF-PREEMPT Alarm	2-50
2.6.53 FAILTOSW	2-51
Clear the FAILTOSW Condition	2-51
2.6.54 FAILTOSW-PATH	2-51
Clear the FAILTOSW-PATH Condition on a UPSR Configuration	2-52
2.6.55 FAILTOSWR	2-53
Clear the FAILTOSWR Condition on a Four-Fiber BLSR Configuration	2-54
2.6.56 FAILTOSWS	2-55
2.6.57 FAN	2-55
Clear the FAN Alarm	2-55
2.6.58 FE-AIS	2-56
Clear the FE-AIS Condition	2-56
2.6.59 FE-DS1-MULTLOS	2-56
Clear the FE-DS1-MULTLOS Condition	2-56
2.6.60 FE-DS1-NSA	2-57
Clear the FE-DS1-NSA Condition	2-57
2.6.61 FE-DS1-SA	2-57
Clear the FE-DS1-SA Condition	2-57
2.6.62 FE-DS1-SNGLLOS	2-58
Clear the FE-DS1-SNGLLOS Condition	2-58
2.6.63 FE-DS3-NSA	2-58
Clear the FE-DS3-NSA Condition	2-58
2.6.64 FE-DS3-SA	2-59
Clear the FE-DS3-SA Condition	2-59
2.6.65 FE-EQPT-NSA	2-59

Clear the FE-EQPT-NSA Condition	2-59
2.6.66 FE-EXERCISING-RING	2-60
2.6.67 FE-EXERCISING-SPAN	2-60
2.6.68 FE-FRCDWKSWPR-RING	2-60
Clear the FE-FRCDWKSWPR-RING Condition	2-60
2.6.69 FE-FRCDWKSWPR-SPAN	2-61
Clear the FE-FRCDWKSWPR-SPAN Condition	2-61
2.6.70 FE-IDLE	2-61
Clear the FE-IDLE Condition	2-61
2.6.71 FE-LOCKOUTOFPR-SPAN	2-62
Clear the FE-LOCKOUTOFPR-SPAN Condition	2-62
2.6.72 FE-LOF	2-62
Clear the FE-LOF Condition	2-62
2.6.73 FE-LOS	2-63
Clear the FE-LOS Condition	2-63
2.6.74 FE-MANWKSWPR-RING	2-63
Clear the FE-MANWKSWPR-RING Condition	2-63
2.6.75 FE-MANWKSWPR-SPAN	2-64
Clear the FE-MANWKSWPR-SPAN Condition	2-64
2.6.76 FEPRLF	2-64
Clear the FEPRLF Alarm on a Four-Fiber BLSR	2-64
2.6.77 FORCED-REQ	2-65
2.6.78 FORCED-REQ-RING	2-65
2.6.79 FORCED-REQ-SPAN	2-65
2.6.80 FRCDSWTOINT	2-65
2.6.81 FRCDSWTOPRI	2-66
2.6.82 FRCDSWTOSEC	2-66
2.6.83 FRCDSWTOTHIRD	2-66
2.6.84 FRNGSYNC	2-66
Clear the FRNGSYNC Alarm	2-66
2.6.85 FSTSYNC	2-67
2.6.86 FULLPASSTHR-BI	2-67
2.6.87 HITEMP	2-67
Clear the HITEMP Alarm	2-68
2.6.88 HLDOVERSYNC	2-68
Clear the HLDOVERSYNC Alarm	2-68
2.6.89 IMPROPRMVL	2-69
Clear the IMPROPRMVL Alarm	2-69
2.6.90 INC-ISD	2-70
2.6.91 INHSWPR	2-70

Clear the INHSWPR Condition	2-71
2.6.92 INHSWWKG	2-71
Clear the INHSWWKG Condition	2-71
2.6.93 INVMACADR	2-71
2.6.94 KB-PASSTHR	2-72
2.6.95 LKOUTPR-S	2-72
2.6.96 LOCKOUT-REQ	2-72
2.6.97 LOCKOUT-REQ-RING	2-72
2.6.98 LOCKOUT-REQ-SPAN	2-72
2.6.99 LOF (BITS)	2-73
Clear the LOF Alarm	2-73
2.6.100 LOF (DS1)	2-74
Clear the LOF Alarm	2-74
2.6.101 LOF (DS3)	2-74
2.6.102 LOF (EC1-12)	2-75
Clear the LOF Alarm	2-75
2.6.103 LOF (OC-N)	2-75
Clear the LOF Alarm	2-75
2.6.104 LOP-P	2-76
Clear the LOP-P Alarm	2-76
2.6.105 LOP-V	2-77
Clear the LOP-V Alarm	2-78
2.6.106 LOS (BITS)	2-79
Clear the LOS Alarm	2-79
2.6.107 LOS (DS-1)	2-79
Clear the LOS Alarm	2-79
2.6.108 LOS (DS-3)	2-80
Clear the LOS Alarm	2-80
2.6.109 LOS (EC1-12)	2-81
Clear the LOS Alarm	2-82
2.6.110 LOS (OC-N)	2-82
Clear the LOS Alarm	2-83
2.6.111 LPBKDS1FEAC	2-84
2.6.112 LPBKDS1FEAC-CMD	2-84
2.6.113 LPBKDS3FEAC	2-85
2.6.114 LPBKDS3FEAC-CMD	2-85
2.6.115 LPBKFACILITY (DS-N or EC1-12)	2-85
Clear the LBKFACILITY Condition	2-86
2.6.116 LPBKFACILITY (OC-N)	2-86
2.6.117 LPBKTERMINAL (DS-N, EC1-12, OC-N)	2-87

2.6.118	LPBKTERMINAL(G1000-4)	2-87
2.6.119	MAN-REQ	2-87
2.6.120	MANRESET	2-88
2.6.121	MANSWTOINT	2-88
2.6.122	MANSWTOPRI	2-88
2.6.123	MANSWTOSEC	2-88
2.6.124	MANSWTOTHIRD	2-89
2.6.125	MANUAL-REQ-RING	2-89
2.6.126	MANUAL-REQ-SPAN	2-89
2.6.127	MEA (AIP)	2-89
2.6.128	MEA (Bplane)	2-89
	Clear the MEA Alarm	2-90
2.6.129	MEA (EQPT)	2-90
	Clear the MEA Alarm	2-90
2.6.130	MEA (FAN)	2-92
	Clear the MEA Alarm	2-92
2.6.131	MEM-GONE	2-93
2.6.132	MEM-LOW	2-93
2.6.133	MFGMEM	2-93
	Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane	2-93
2.6.134	PDI-P	2-94
	Clear the PDI-P Condition	2-95
2.6.135	PEER-NORESPONSE	2-96
	Clear the PEER-NORESPONSE Alarm	2-96
2.6.136	PLM-P	2-96
	Clear the PLM-P Alarm	2-97
2.6.137	PLM-V	2-98
	Clear the PLM-V Alarm	2-98
2.6.138	PRC-DUPID	2-98
	Clear the PRC-DUPID Alarm	2-98
2.6.139	PROTNA	2-99
	Clear the PROTNA Alarm	2-99
2.6.140	PWR-A	2-100
	Clear the PWR-A Alarm	2-100
2.6.141	PWR-B	2-100
	Clear the PWR-B Alarm	2-100
2.6.142	RAI	2-101
2.6.143	RCVR-MISS	2-101
	Clear the RCVR-MISS Alarm	2-101
2.6.144	RFI-L	2-102

Clear the RFI-L Condition	2-102
2.6.145 RFI-P	2-102
Clear the RFI-P Condition	2-102
2.6.146 RFI-V	2-103
Clear the RFI-V Condition	2-103
2.6.147 RING-MISMATCH	2-104
Clear the RING-MISMATCH Alarm	2-104
2.6.148 RING-SW-EAST	2-104
2.6.149 RING-SW-WEST	2-104
2.6.150 SD-L	2-105
Clear the SD-L Condition	2-105
2.6.151 SD-P	2-106
Clear the SD-P Condition	2-107
2.6.152 SF-L	2-107
Clear the SF-L Condition	2-108
2.6.153 SF-P	2-108
Clear the SF-P Condition	2-109
2.6.154 SFTWDOWN	2-110
2.6.155 SNTP-HOST	2-110
Clear the SNTP-HOST Alarm	2-110
2.6.156 SPAN-SW-EAST	2-110
2.6.157 SPAN-SW-WEST	2-111
2.6.158 SQUELCH	2-111
Clear the SQUELCH Condition	2-111
2.6.159 SSM-DUS	2-112
2.6.160 SSM-FAIL	2-113
Clear the SSM-FAIL Alarm	2-113
2.6.161 SSM-OFF	2-113
2.6.162 SSM-PRS	2-113
2.6.163 SSM-RES	2-114
2.6.164 SSM-SMC	2-114
2.6.165 SSM-ST2	2-114
2.6.166 SSM-ST3	2-114
2.6.167 SSM-ST3E	2-115
2.6.168 SSM-ST4	2-115
2.6.169 SSM-STU	2-115
Clear the STU Condition	2-116
2.6.170 SSM-TNC	2-116
2.6.171 SWMTXMOD	2-116
Clear the SWMTXMOD Alarm	2-116

2.6.172	SWTOPRI	2-118
2.6.173	SWTOSEC	2-118
2.6.174	SWTOTHIRD	2-118
2.6.175	SYNC-FREQ	2-118
	Clear the SYNC-FREQ Condition	2-118
2.6.176	SYNCPRI	2-119
	Clear the SYNCPRI Alarm	2-119
2.6.177	SYNCSEC	2-119
	Clear the SYNCSEC Alarm	2-120
2.6.178	SYNCTHIRD	2-120
	Clear the SYNCTHIRD Alarm	2-120
2.6.179	SYSBOOT	2-121
2.6.180	TIM-P	2-121
	Clear the TIM-P Alarm	2-121
2.6.181	TPTFAIL	2-122
	Clear the TPTFAIL Alarm	2-122
2.6.182	TRMT	2-122
	Clear the TRMT Alarm	2-123
2.6.183	TRMT-MISS	2-123
	Clear the TRMT-MISS Alarm	2-123
2.6.184	UNEQ-P	2-124
	Clear the UNEQ-P Alarm	2-124
2.6.185	UNEQ-V	2-125
	Clear the UNEQ-V Alarm	2-126
2.6.186	WKSWPR	2-127
2.6.187	WTR	2-127
2.7	DS3-12E Line Alarms	2-127
2.8	Common Procedures in Alarm Troubleshooting	2-129
	Identify a Ring ID or Node ID Number	2-129
	Change a Ring ID Number	2-129
	Change a Node ID Number	2-129
	Verify Node Visibility for Other Nodes	2-130
	Check or Create Node SDCC Terminations	2-130
	Lock Out a BLSR Span	2-130
	Clear a BLSR Span Command	2-130
	Clear a UPSR Lockout	2-131
	Move Protection Group Traffic with a Switch Command	2-131
	Side Switch the Active or Standby Cross-Connect Card	2-131
	Clear a Protection Group Switch Command	2-132
	Delete a Circuit	2-132

- Clear a Loopback 2-132
- Reset the Active TCC+ Card in CTC 2-133
- Reset a Traffic Card in CTC 2-133
- Verify BER Threshold Level 2-133
- Physically Replace a Card 2-134
- Remove and Reinsert (Reseat) a Card 2-134
- Remove and Reinsert Fan Tray 2-134

CHAPTER 3**Replace Hardware 3-1**

- 3.1 Switch Traffic and Replace an In-Service Cross-Connect Card 3-1
- 3.2 Remove and Reinsert (Reseat) the Standby TCC+ 3-4
- 3.3 Replace the Air Filter 3-5
 - 3.3.1 Inspect, Clean, and Replace the Reusable Air Filter 3-5
 - 3.3.2 Inspect and Replace the Disposable Air Filter 3-7
- 3.4 Determine Replacement Hardware Compatibility 3-9
- 3.5 Replace the Fan-Tray Assembly 3-11
- 3.6 Replace the Alarm Interface Panel 3-13
- 3.7 Replace the Electrical Interface Assembly 3-19

CHAPTER 4**Error Messages Troubleshooting 4-1**

- 4.1 Circuit Errors 4-1
 - 4.1.1 Circuit Source Error 4-1
 - 4.1.1.1 Exception: Source node must be selected 4-1
 - 4.1.1.2 Exception: Source is not fully specified 4-2
 - 4.1.1.3 Exception: Secondary Source is not fully specified 4-2
 - 4.1.1.4 Exception: Sources can't be identical 4-2
 - 4.1.2 Circuit Destination Error 4-3
 - 4.1.2.1 Exception: Destination node must be selected 4-3
 - 4.1.2.2 Exception: Destination is not fully specified 4-3
 - 4.1.2.3 Exception: Secondary Destination is not fully specified 4-3
 - 4.1.2.4 Exception: Destinations can't be identical 4-3
 - 4.1.3 Circuit Destroy Failed 4-4
 - 4.1.3.1 CmsCommFailException: < node-ip address > Communications error (COMM_FAILURE) while attempting to set the CircuitModel.delete attribute 4-4
 - 4.1.3.2 CmsCommFailException: < node-ip address > The Node was not initialized while attempting to set the CircuitModel.delete attribute 4-4
 - 4.1.4 Auto-Ranging Circuit Creation 4-5

- 4.1.4.1 Unable to provision circuit Unexpected exception encountered Attempts to access a VtAdit that has been destroyed.CmsObjectNotExistException: Attempts to access a VtAdit that has been destroyed. **4-5**
- 4.1.4.2 NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements. **4-5**
- 4.1.4.3 Unable to drop route ComputeRouteInMixedDomains: No Route found with given requirements NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements **4-6**
- 4.1.4.4 NoRoute: Unable to route VT Circuit: possible reasons: 1) VT Tunnel required and cannot route due to XCs in the path from source to destination 2) Cannot find route that satisfies given requirements **4-7**
- 4.1.4.5 Exception: Source is not fully specified **4-8**
- 4.1.5 Node Selection Error **4-8**
 - 4.1.5.1 Failure getting list of available ports from <node-name> <node ipaddress> Communications error (COMM_FAILURE) while attempting to get the ConnectionModels.availEntitiesForVtsPath attribute. **4-8**
- 4.1.6 Circuit Creation Error **4-9**
 - 4.1.6.1 Circuit creation cannot proceed due to changes in the network, which affect the circuit(s) being created. The dialog will close. Please try again. **4-9**
- 4.1.7 Error While finishing Circuit Creation **4-9**
 - 4.1.7.1 Unable to provision circuit No VT-capable STSs are available at <node-name> **4-9**
 - 4.1.7.2 Unable to provision circuit Circuit provision error Unable to create connection at <node-name> **4-10**
 - 4.1.7.3 NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements. **4-10**
 - 4.1.7.4 Circuit sanity check failed. Invalid connection at node <node name> SanityCheckFailed: Invalid connection at node <node name>. **4-11**
 - 4.1.7.5 CmsObjectNotExistException: Atmpt to access the CtAditModel.getAvailableSts attribute for an object that does not exist. **4-11**
 - 4.1.7.6 Circuit spans verification: selected spans are invalid! Invalid span combination at Node <node name> SanityCheckFailed: Invalid span combination at Node <node name> **4-11**
 - 4.1.7.7 Circuit spans verification" selected spans are invalid! Link Diverse Path requirement is not met. The link is <node name source -> <node name destination> (LINK_VTT unprot, State=Up). Node Check is the link is a VT Tunnel **4-12**
 - 4.1.7.8 Circuit sanity check failed. Path specified is not protected. Check span <node name> -> <nodename> (LINK_PHYSICAL unprot, State=Up). OCN IsmState=2,2. **4-12**
 - 4.1.7.9 Circuit sanity check failed. Source/Drop is an endpoint of a network link. **4-12**
 - 4.1.7.10 Unable to route drop. ComputerRouteInMixedDomains: No Route found with given requirements. NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements **4-13**
- 4.1.8 Error Adding Drop **4-14**
 - 4.1.8.1 SanityCheckFailed: Source/Drop is an endpoint of a network link **4-14**
 - 4.1.8.2 Exception: Drop node must be selected **4-14**

- 4.1.8.3 Circuit provisioning error Unable to add output to connection at <node-name> Path already in use **4-14**
- 4.1.9 Error Applying Changes **4-15**
 - 4.1.9.1 InvalidProtectionOp: Unable to switch. A higher priority request may be present. **4-15**
- 4.1.10 Error Deleting Circuit Drop **4-15**
 - 4.1.10.1 IncorrectCircuitState: Circuit drop can be deleted only when state is CREATING, ACTIVE or DROP_PENDING **4-15**
 - 4.1.10.2 CannotDeleteLastDrop: Last circuit drop cannot be deleted. Please destroy the circuit instead **4-15**
- 4.1.11 Error **4-16**
 - 4.1.11.1 Please select a node first **4-16**
 - 4.1.11.2 This link may not be included in the required list. Constraints only apply to the primary path. **4-16**
 - 4.1.11.3 This node is not selectable: Only the Source node and nodes attached to included (blue) are selectable. Selecting a selectable node will enable its available outgoing spans **4-16**
 - 4.1.11.4 This span is not selectable. Only green spans with arrows. **4-17**
 - 4.1.11.5 Sorry, no paths are available on this link. Please make another selection. **4-17**
 - 4.1.11.6 This link may not be included in the required list. Only 1 outgoing link may be included for each node. **4-17**
- 4.1.12 Circuit Deletion Error **4-18**
 - 4.1.12.1 DeletionError: Following Circuits Could Not Be Scheduled for Deletion . Error deleting circuit TUN_<node name> ::10:cerent.cms.ncp. SanityCheckFailed: VT Tunnel is in use. **4-18**
- 4.1.13 Circuit Attributes Error **4-18**
 - 4.1.13.1 Exception: Circuit name is too long(max 48)) **4-18**
 - 4.1.13.2 NumberFormatException **4-18**
 - 4.1.13.3 NumberFormatException:999999999999999 **4-19**
 - 4.1.13.4 Exception: Number of Circuit must be a positive integer **4-19**
- 4.1.14 Error Validating Slot Number **4-19**
 - 4.1.14.1 Please enter a valid value for the Slot Number **4-19**
- 4.1.15 Error Validating Port Number **4-19**
 - 4.1.15.1 Please enter a valid value for the Port Number **4-20**
- 4.1.16 Circuit Route Constraints Error **4-20**
 - 4.1.16.1 Unable to route drop Compute. RouteInMixedDomains: No Route found with given requirements. NoRoute: ComputeRouteInMixedDomains: No Route found with given requirements. **4-20**
- 4.2 BLSR Errors **4-21**
 - 4.2.1 Cannot Delete Ring **4-21**
 - 4.2.1.1 There is a protection operation set. All protection operations must be clear for ring to be deleted. **4-21**
 - 4.2.2 Invalid Ring ID **4-21**
 - 4.2.2.1 RingID must be an integer between 0 and 9999 **4-22**
 - 4.2.3 Error **4-22**

4.2.3.1	The Ring ID value is not valid . Please enter a valid number between 0 and 9999.	4-22
4.2.3.2	Cannot set reversion to INCONSISTENT!	4-22
4.2.3.3	You must enter a number and it must be between 0 and 31.	4-22
4.2.3.4	Error - this node ID is already in use. Please choose another.	4-23
4.2.4	Error Applying Changes	4-23
4.2.4.1	Exception: Unable to switch East Line, a higher priority request may be present.	4-23
4.2.4.2	Exception: Unable to switch West Line, a higher priority request may be present.	4-23
4.2.5	Duplicate Node ID	4-24
4.2.5.1	New Node ID (N) for Ring ID N duplicate ID of node <ip address>	4-24
4.2.6	BLSR Error	4-24
4.2.6.1	Exception: West and East ports must be different	4-24
4.2.6.2	Exception: West and East ports must have the same line rate	4-25
4.2.6.3	Exception: Unable to parse Ring ID	4-25

INDEX



FIGURES

Figure 1-1	The facility loopback process on a DS-N card	1-2
Figure 1-2	The facility loopback process on an OC-N card	1-2
Figure 1-3	The terminal loopback process on an OC-N card	1-3
Figure 1-4	The terminal loopback process on a DS-N card	1-3
Figure 1-5	The hairpin circuit process on a DS-N card	1-3
Figure 1-6	A facility loopback on a circuit source DS-N port	1-4
Figure 1-7	Hairpin on a source node port	1-8
Figure 1-8	Terminal loopback on a destination DS-N port	1-11
Figure 1-9	Hairpin on a destination node	1-14
Figure 1-10	Facility loopback on a destination DS-N port	1-17
Figure 1-11	Accessing FEAC functions on the DS3XM-6 card	1-21
Figure 1-12	Diagram of FEAC	1-22
Figure 1-13	A facility loopback on a circuit source OC-N port	1-23
Figure 1-14	Terminal loopback on a source-node OC-N port	1-25
Figure 1-15	Facility loopback on an intermediate-node OC-N port	1-28
Figure 1-16	Terminal loopback on an intermediate-node OC-N port	1-31
Figure 1-17	Facility loopback on a destination-node OC-N port	1-34
Figure 1-18	Terminal loopback on a destination-node OC-N port	1-37
Figure 1-19	Reinitialization tool in Windows	1-42
Figure 1-20	Confirm NE Restoration	1-43
Figure 1-21	The reinitialization tool in UNIX	1-44
Figure 1-22	Deleting the CTC cache	1-52
Figure 1-23	Ethernet connectivity reference	1-59
Figure 1-24	A VLAN with Ethernet ports at Tagged and Untag	1-60
Figure 1-25	Configuring VLAN membership for individual Ethernet ports	1-62
Figure 1-26	A gigabit interface converter (GBIC)	1-73
Figure 1-27	Installing a GBIC on the E1000-2/E1000-2-G card	1-75
Figure 1-28	RJ-45 pin numbers	1-76
Figure 1-29	LAN cable layout	1-76
Figure 1-30	Cross-over cable layout	1-77
Figure 3-1	A reusable fan-tray air filter in an external filter bracket (front door removed)	3-6

<i>Figure 3-2</i>	Inserting or removing the fan-tray assembly (front door removed)	3-8
<i>Figure 3-3</i>	Inserting or removing a disposable fan-tray air filter (front door removed)	3-9
<i>Figure 3-4</i>	Removing or replacing the fan-tray assembly (front door removed)	3-13
<i>Figure 3-5</i>	Find the MAC address	3-14
<i>Figure 3-6</i>	Lower backplane cover	3-15
<i>Figure 3-7</i>	Repair Circuits in the Menu Bar	3-17
<i>Figure 3-8</i>	Repairing circuits	3-17
<i>Figure 3-9</i>	Recording the old MAC address before replacing the AIP	3-18
<i>Figure 3-10</i>	Circuit repair information	3-18
<i>Figure 4-1</i>	An error dialog box	4-1



TABLES

<i>Table 1-1</i>	Restore the Node Database	1-40
<i>Table 1-2</i>	Restore the Node to Factory Configuration	1-41
<i>Table 1-3</i>	Unable to Verify the IP Configuration of your PC	1-45
<i>Table 1-4</i>	Browser Login Does Not Launch Java	1-46
<i>Table 1-5</i>	Unable to Verify the NIC Connection on your PC	1-48
<i>Table 1-6</i>	Verify PC connection to ONS 15454 (ping)	1-48
<i>Table 1-7</i>	Browser Stalls When Downloading Files From TCC+	1-49
<i>Table 1-8</i>	Browser Stalls When Downloading jar File From TCC+	1-50
<i>Table 1-9</i>	CTC Does Not Launch	1-51
<i>Table 1-10</i>	Sluggish CTC Operation or Login Problems	1-52
<i>Table 1-11</i>	Node Icon is Grey on CTC Network View	1-53
<i>Table 1-12</i>	CTC Cannot Launch Due to Applet Security Restrictions	1-54
<i>Table 1-13</i>	Java Runtime Environment Incompatible	1-55
<i>Table 1-14</i>	JRE Compatibility	1-55
<i>Table 1-15</i>	Different CTC Releases Do Not Recognize Each Other	1-56
<i>Table 1-16</i>	Username or Password Do Not Match	1-57
<i>Table 1-17</i>	No IP Connectivity Exists Between Nodes	1-57
<i>Table 1-18</i>	DCC Connection Lost	1-58
<i>Table 1-19</i>	"Path in Use" error when creating a circuit	1-58
<i>Table 1-20</i>	Calculate and Design IP Subnets	1-58
<i>Table 1-21</i>	Calculate and Design IP Subnets	1-59
<i>Table 1-22</i>	Verify PC connection to ONS 15454 (ping)	1-61
<i>Table 1-23</i>	Cross-Connect Card Oscillator Fails	1-63
<i>Table 1-24</i>	Circuit in Partial State	1-65
<i>Table 1-25</i>	Calculate and Design IP Subnets	1-66
<i>Table 1-26</i>	Circuit Creation Error with VT1.5 Circuit	1-67
<i>Table 1-27</i>	Unable to Create Circuit from DS-3 Card to DS3XM-6 Card	1-67
<i>Table 1-28</i>	DS3 Card Does Not Report AIS-P From External Equipment	1-67
<i>Table 1-29</i>	OC-3 and DCC Limitations	1-68
<i>Table 1-30</i>	ONS 15454 Switches Timing Reference	1-68
<i>Table 1-31</i>	Holdover Synchronization Alarm	1-69

<i>Table 1-32</i>	Free-Running Synchronization Mode	1-69
<i>Table 1-33</i>	Daisy-Chained BITS Not Functioning	1-69
<i>Table 1-34</i>	Blinking STAT LED on installed card	1-70
<i>Table 1-35</i>	Bit Errors Appear for a Line Card	1-71
<i>Table 1-36</i>	Faulty Fiber-Optic Connections	1-71
<i>Table 1-37</i>	LAN cable pinout	1-76
<i>Table 1-38</i>	Cross-over cable pinout	1-77
<i>Table 1-39</i>	Optical Card Transmit and Receive Levels	1-77
<i>Table 1-40</i>	Power Supply Problems	1-78
<i>Table 1-41</i>	Power Consumption for Node and Cards	1-79
<i>Table 1-42</i>	Lamp Test for Card LEDs	1-80
<i>Table 2-1</i>	Critical Alarm Index	2-1
<i>Table 2-2</i>	Major Alarm Index	2-2
<i>Table 2-3</i>	Minor Alarm Index	2-2
<i>Table 2-4</i>	Conditions Index	2-3
<i>Table 2-5</i>	Alarm Index	2-4
<i>Table 2-6</i>	Alarm Index by Alarm Type	2-6
<i>Table 2-7</i>	Alarm Type/Object Definition	2-13
<i>Table 2-8</i>	DS3-12E Line Alarms	2-128
<i>Table 3-1</i>	Incompatibility Alarms	3-10



About this Manual

The *Cisco ONS 15454 Troubleshooting Guide* provides troubleshooting procedures for SONET alarms and error messages, and provides symptoms and solutions for general troubleshooting problems such as CTC and hardware errors. This guide also contains hardware replacement procedures.

To install, turn up, provision, and maintain a Cisco ONS 15454 node and network, refer to the *Cisco ONS 15454 Procedure Guide*. For explanation and information, refer to the *Cisco ONS 15454 Reference Manual*.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at this URL:

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

Documentation CD-ROM

Optical networking-related documentation is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated monthly and may be more current than printed documentation.

Ordering Documentation

You can order Cisco documentation in these ways:

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

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

<http://www.cisco.com/tac>

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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



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 2, “Alarm Troubleshooting.”](#) If you cannot find what you are looking for contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

This chapter includes 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.



Note For network acceptance tests, refer to the *Cisco ONS 15454 Procedures Guide*.

- [Identify Points of Failure on a DS-N Circuit Path](#)—Explains how to perform the tests described in the “Network Troubleshooting Tests” section on a DS-N circuit.
- [Using the DS3XM-6 Card FEAC \(Loopback\) Functions](#)—Describes the Far End Alarm and Control (FEAC) functions on the DS3XM-6 card.
- [Identify Points of Failure on an OC-N Circuit Path](#)—Explains how to perform the tests described in the “Network Troubleshooting Tests” section on an OC-N circuit.

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

- [Restoring the Database and Default Settings](#)—Provides procedures for restoring software data and restoring the node to the default setup.
- [PC Connectivity Troubleshooting](#)—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454
- [CTC Operation Troubleshooting](#)—Provides troubleshooting procedures for CTC log-in or operation problems.
- [Circuits and Timing](#)—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- [Fiber and Cabling](#)—Provides troubleshooting procedures for fiber and cabling connectivity errors.

1.1 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.

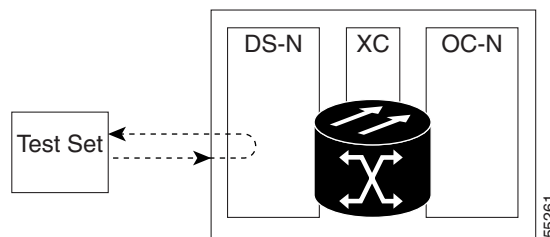


Caution

On OC-N cards, a facility 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 port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or cabling plant as the potential cause of a network problem. [Figure 1-1](#) shows a facility loopback on a DS-N card.

Figure 1-1 The facility loopback process on a DS-N card



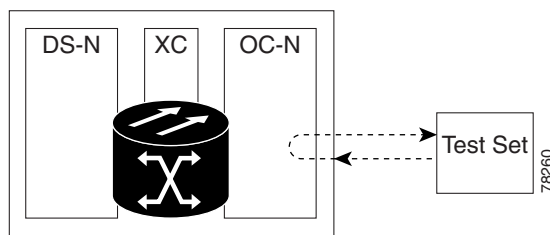
To test the LIU on an OC-N card, connect an optical test set to the OC-N port and perform a facility loopback or use a loopback or hairpin on a card that is farther along the circuit path. [Figure 1-2](#) shows a facility loopback on an OC-N card.



Caution

Before performing a facility loopback on an OC-N card, make sure the card contains at least two DCC paths to the node where the card is installed. A second DCC 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 DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N card.

Figure 1-2 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 loops back from the card with the loopback. [Figure 1-3](#) 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 back through the cross-connect card to the DS-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the OC-N card.

Figure 1-3 The terminal loopback process on an OC-N card

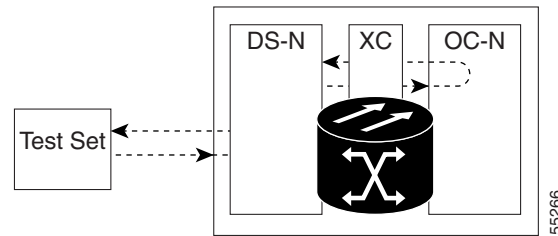
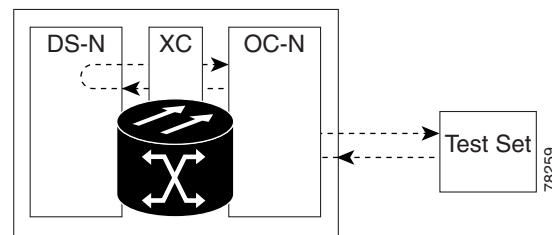


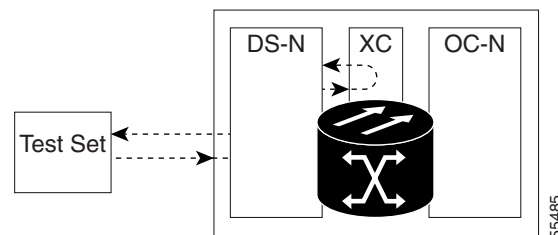
Figure 1-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the OC-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the DS-N card.

Figure 1-4 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 specific STS or VT circuit on nodes running live traffic.

Figure 1-5 The hairpin circuit process on a DS-N card



1.2 Identify Points of Failure on a DS-N Circuit Path

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

The example in this section tests 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 are tested and eliminated. A logical progression of five network test procedures apply to this example 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
2. A hairpin on the source-node DS-N
3. A terminal loopback on the destination-node DS-N
4. A hairpin on the destination-node DS-N
5. A facility loopback on the destination DS-N

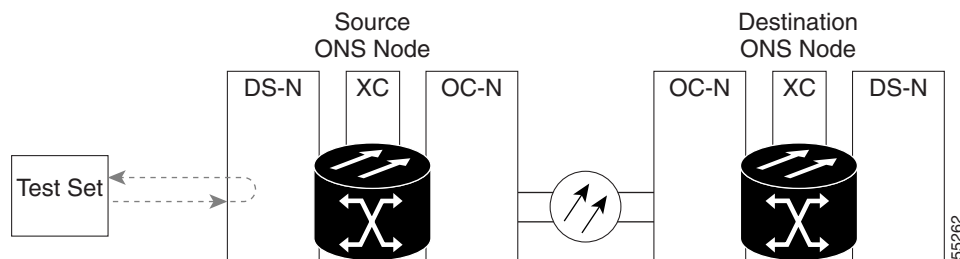

Note

All loopback tests require on-site personnel.

1.2.1 Perform a Facility Loopback on a Source DS-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the DS-N port in the source node. Completing a successful facility loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. [Figure 1-6](#) shows an example of a facility loopback on a source DS-N port.

Figure 1-6 A facility loopback on a circuit source DS-N port


Caution

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

Procedure: Create the Facility Loopback on the Source DS-N port

- 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 on the port being tested:
- In node view, double-click the card where you will perform the loopback.
 - Click the **Maintenance > Loopback** tabs.
 - Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.
 - Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

- Step 3** Proceed to the [“Test the Facility Loopback Circuit”](#) section on page 1-5.

Procedure: Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.
- Proceed to the [“Perform a Hairpin on a Source Node Port”](#) section on page 1-8.
- 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.
- Proceed to the [“Test the DS-N Cabling”](#) section on page 1-6.

Procedure: 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.
- 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 defective.
- Step 2** Resend test traffic on the loopback circuit with a known-good cable installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective cable.
Replace the defective cable.
Clear the facility loopback before testing the next segment of the network circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - d. Click the **Apply** button.
 - e. Click the **Yes** button in the Confirmation Dialog box.
- Proceed to the [“Perform a Hairpin on a Source Node Port”](#) section on page 1-8.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty EIA.
Proceed to the [“Test the DS-N Card”](#) section on page 1-6.
-

Procedure: Test the DS-N Card

-
- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- Step 2** Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
Replace the faulty card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.
Clear the facility loopback before testing the next segment of the network circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

- d. Click the **Apply** button.
- e. Click the **Yes** button in the Confirmation Dialog box.

Proceed to the “[Perform a Hairpin on a Source Node Port](#)” section on page 1-8.

Step 4 If the test set indicates a faulty circuit, the problem may be a faulty EIA.

Proceed to the “[Test the EIA](#)” section on page 1-7.

Procedure: 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 “[Replace the Electrical Interface Assembly](#)” section on page 3-19.
- 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. Clear the facility loopback before testing the next segment of the network circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - d. Click the **Apply** button.
 - e. Click the **Yes** button in the Confirmation Dialog box.
- Proceed to the “[Perform a Hairpin on a Source Node Port](#)” section on page 1-8
- Step 4** If the test set indicates a faulty circuit, the problem is probably a defective EIA.
- a. Return the defective EIA to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
 - b. Replace the faulty EIA. See [Chapter 3, “Replace Hardware”](#) for details.
- 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. Clear the facility loopback before testing the next segment of the circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

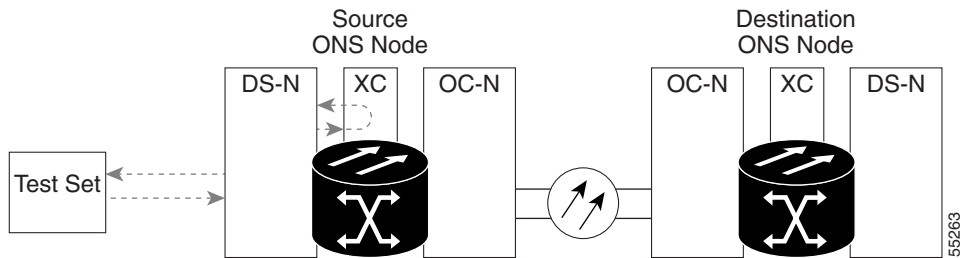
- d. Click the **Apply** button.
- e. Click the **Yes** button in the Confirmation Dialog box.

Proceed to the “[Perform a Hairpin on a Source Node Port](#)” section on page 1-8.

1.2.2 Perform a Hairpin on a Source Node Port

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. [Figure 1-7](#) shows an example of a hairpin loopback on a source node port.

Figure 1-7 Hairpin on a source node port



Note

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

Procedure: Create the Hairpin on the Source Node Port

- 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 Port](#)” section on page 1-4, leave the electrical test set hooked up to the DS-N port in the source node.
 - b. If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the 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 the **Next** button.
 - e. In the Circuit Source dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

- f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 1-way circuit.
- Step 4** Proceed to the [“Test the Hairpin Circuit”](#) section on page 1-9
-

Procedure: Test the Hairpin Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit before testing the next segment of the network circuit path.
- a. Click the **Circuits** tab.
 - b. Choose the hairpin circuit being tested.
 - c. Click the **Delete** button.
 - d. Click the **Yes** button in the Delete Circuits box.
 - e. Confirm that the hairpin circuit is deleted from the Circuits tab list.
- Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Port”](#) section on page 1-11.
- Step 4** If the test set indicates a faulty circuit, there may be a problem with the cross-connect card. Proceed to the [“Test the Standby Cross-Connect Card”](#) section on page 1-9.
-

Procedure: 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. In the Cross Connect Cards menu, click the **Switch** button.

- d. Click the **Yes** button in the Confirm Switch box.



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

Step 3 Resend test traffic on the loopback circuit.

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

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

Clear the hairpin circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the hairpin circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.
- e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Proceed to the “[Perform a Terminal Loopback on a Destination DS-N Port](#)” section on page 1-11.

Step 5 If the test set indicates a good circuit, the problem may be a defective cross-connect card.

To confirm a defective original cross-connect card, proceed to the “[Retest the Original Cross-Connect Card](#)” section on page 1-10.

Procedure: Retest the Original Cross-Connect Card

Step 1 Do a manual switch (side switch) of the cross-connect cards to make the original cross-connect card the active card.

- a. Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
- b. In node view, select the **Maintenance > XC Cards** tabs.
- c. From the Cross Connect Cards menu, choose **Switch**.
- d. Click the **Yes** button in the Confirm Switch box.

Step 2 Resend test traffic on the loopback circuit.

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the defective cross-connect card. See [Chapter 3, “Replace Hardware”](#) for details.

Clear the hairpin circuit before testing the next segment of the network circuit path.

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

- d. Click the **Yes** button in the Delete Circuits box.
- e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Port”](#) section on page 1-11

Step 4 If the test set indicates a good circuit, the cross-connect card may have had a temporary problem that was cleared by the side switch.

Clear the hairpin circuit before testing the next segment of the network circuit path.

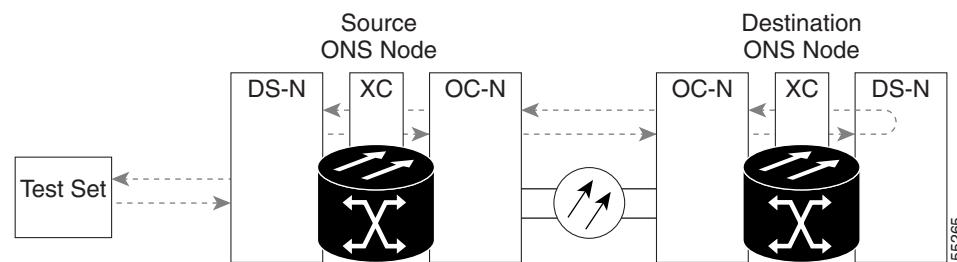
- a. Click the **Circuits** tab.
- b. Choose the hairpin circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.
- e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Port”](#) section on page 1-11.

1.2.3 Perform a Terminal Loopback on a Destination DS-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the DS-N port in the destination node. First, create a bidirectional circuit that starts on the source node DS-N port and loops back 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 port verifies that the circuit is good up to the destination DS-N. [Figure 1-8](#) shows an example of a terminal loopback on a destination DS-N port.

Figure 1-8 Terminal loopback on a destination DS-N port



Caution

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

Procedure: Create the Terminal Loopback on a Destination DS-N Port

- 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 Port”](#) section on page 1-8, leave the electrical test set hooked up to the DS-N port in the source node.

- b. If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the 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 the **Next** button.
 - e. In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the DS-N port in the destination node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.



Note It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 4** Create the terminal loopback on the destination port being tested:
- a. Go to the node view of the destination node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down list in the Select Node box and click the **OK** button.
 - b. In node view, double-click the card that requires the loopback, such as the DS-N card in the destination node.
 - c. Click the **Maintenance > Loopback** tabs.
 - d. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
 - e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - f. Click the **Apply** button.
 - g. Click the **Yes** button in the Confirmation Dialog box.
- Step 5** Proceed to the “[Test the Terminal Loopback Circuit on the Destination DS-N Port](#)” section on page 1-12.
-

Procedure: Test the Terminal Loopback Circuit on the Destination DS-N Port

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit.

Clear the terminal loopback before testing the next segment of the network circuit path.

- a. Double-click the DS-N card in the destination node with the terminal loopback.
- b. Click the **Maintenance > Loopback** tabs.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “[Perform a Hairpin on a Destination Node](#)” section on page 1-14.

- 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 1-13.

Procedure: Test the Destination DS-N Card

- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Replace the defective DS-N card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the terminal loopback before testing the next segment of the network circuit path.

- a. Double-click the DS-N card in the destination node with the terminal loopback.
- b. Click the **Maintenance > Loopback** tabs.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

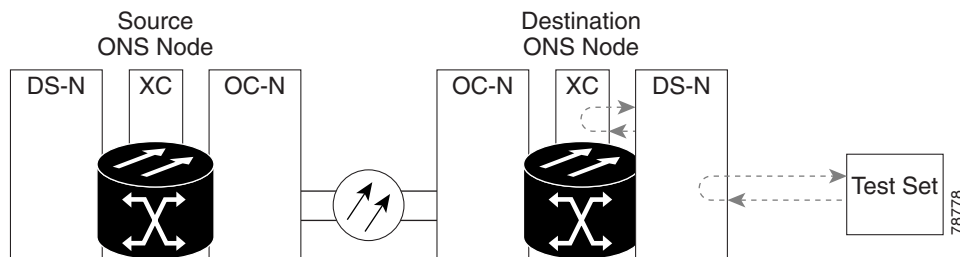
- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “[Perform a Hairpin on a Destination Node](#)” section on page 1-14.

1.2.4 Perform a Hairpin on a Destination 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 isolates the possibility that the cross-connect card is the cause of the faulty circuit. [Figure 1-7](#) shows an example of a hairpin loopback on a destination node.

Figure 1-9 Hairpin on a destination 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.

Procedure: Create the Hairpin on the Destination Node

- 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 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 the **Next** button.
 - e. In the Circuit Source dialog box, select the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.

- f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears in the Circuits tab list as a 1-way circuit.
- Step 4** Proceed to the [“Test the Hairpin Circuit” section on page 1-15](#)
-

Procedure: Test the Hairpin Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit before testing the next segment of the network circuit path.
- a. Click the **Circuits** tab.
 - b. Choose the hairpin circuit being tested.
 - c. Click the **Delete** button.
 - d. Click the **Yes** button in the Delete Circuits box.
 - e. Confirm that the hairpin circuit is deleted from the Circuits tab list.
- Proceed to the [“Perform a Facility Loopback on a Destination DS-N Port” section on page 1-17](#).
- Step 4** If the test set indicates a faulty circuit, there may be a problem with the cross-connect card. Proceed to the [“Test the Standby Cross-Connect Card” section on page 1-15](#).
-

Procedure: 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. In the Cross Connect Cards menu, click the **Switch** button.

- d. Click the **Yes** button in the Confirm Switch box.



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

Step 3 Resend test traffic on the loopback circuit.

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

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

Clear the hairpin circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the hairpin circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.
- e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Proceed to the “[Perform a Facility Loopback on a Destination DS-N Port](#)” section on page 1-17.

Step 5 If the test set indicates a good circuit, the problem may be a defective cross-connect card.

To confirm a defective original cross-connect card, proceed to the “[Retest the Original Cross-Connect Card](#)” section on page 1-16.

Procedure: Retest the Original Cross-Connect Card

Step 1 Do a manual switch (side switch) of the cross-connect cards to make the original cross-connect card the active card.

- a. Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
- b. In node view, select the **Maintenance > XC Cards** tabs.
- c. In the Cross Connect Cards menu, click the **Switch** button.
- d. Click the **Yes** button in the Confirm Switch box.

Step 2 Resend test traffic on the loopback circuit.

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the defective cross-connect card. See [Chapter 3, “Replace Hardware”](#) for details.

Clear the hairpin circuit before testing the next segment of the network circuit path.

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

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

Proceed to the [“Perform a Facility Loopback on a Destination DS-N Port”](#) section on page 1-17

- Step 4** If the test set indicates a good circuit, the cross-connect card may have had a temporary problem that was cleared by the side switch.

Clear the hairpin circuit before testing the next segment of the network circuit path.

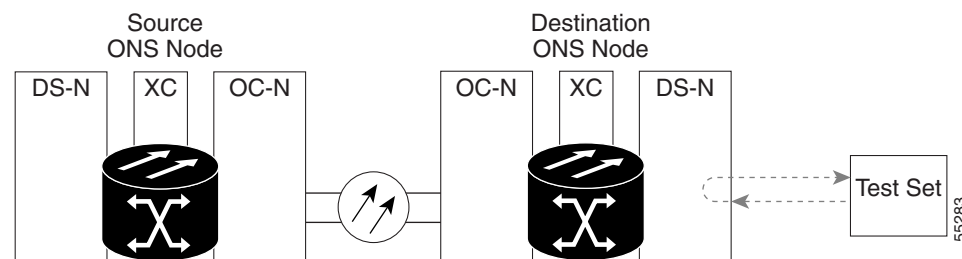
- a. Click the **Circuits** tab.
- b. Choose the hairpin circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the [“Perform a Facility Loopback on a Destination DS-N Port”](#) section on page 1-17.

1.2.5 Perform a Facility Loopback on a Destination DS-N Port

The facility loopback test is performed on the node source port in the circuit, in this example, the destination DS-N port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination node cabling, DS-N card, LIU, or EIA is responsible for a faulty circuit. [Figure 1-10](#) shows an example of a facility loopback on a destination DS-N port.

Figure 1-10 Facility loopback on a destination DS-N port



Caution

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

Procedure: Create a Facility Loopback Circuit on a Destination DS-N Port

- Step 1** Connect an electrical test set to the port you are testing:
- a. If you just completed the [“Perform a Hairpin on a Destination Node”](#) section on page 1-14, leave the electrical test set hooked up to the DS-N port in the destination node.
 - b. If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the 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 create the facility loopback on the port being tested:
- In node view, double-click the card where the loopback will be performed.
 - Click the **Maintenance > Loopback** tabs.
 - 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.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

- Step 3** Proceed to the [“Test the Facility Loopback Circuit” section on page 1-18](#).

Procedure: Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the loopback circuit. Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.

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. Proceed to the [“Test the DS-N Cabling” section on page 1-18](#).

Procedure: 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.
- 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 defective.

- Step 2** Resend test traffic on the loopback circuit with a known-good cable installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective cable.
Replace the defective cable.
Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.
- 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 card or a faulty EIA.
Proceed to the “[Test the DS-N Card](#)” section on page 1-19.
-

Procedure: Test the DS-N Card

- Step 1** Replace the suspect card with a known-good card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- Step 2** Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
Replace the faulty card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.
Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.
- 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.

Proceed to the “[Test the EIA](#)” section on page 1-20.

Procedure: Test the EIA

- Step 1** Remove and reinstall the EIA to ensure a proper seating.
- Remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454, and pull it away from the shelf assembly.
 - Loosen the nine perimeter screws that hold the EIA panel in place.
 - Lift the EIA panel by the bottom to remove it from the shelf assembly.
 - Follow the installation procedure for the appropriate EIA. See the “[Replace the Electrical Interface Assembly](#)” section on page 3-19 for details.
- 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.
- Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.
- 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.
- Return the defective EIA to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
 - Replace the faulty EIA. See [Chapter 3, “Replace Hardware”](#) for details.
- 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, contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
- Step 7** If the test set indicates a good circuit, the problem was probably the defective EIA.
- Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.

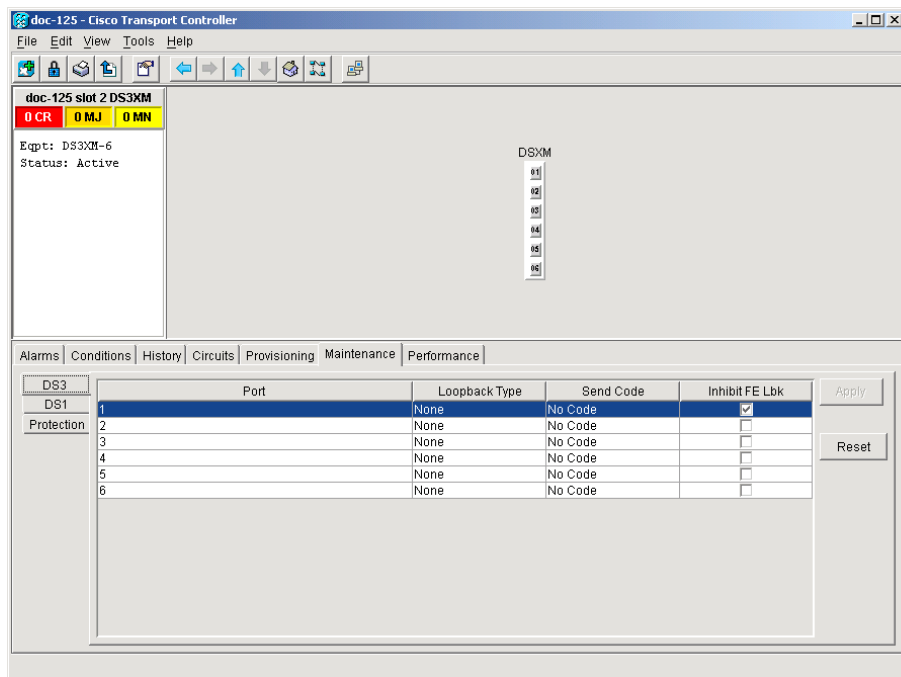
- e. Click the **Yes** button in the Confirmation Dialog box.

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

1.3 Using the DS3XM-6 Card FEAC (Loopback) Functions

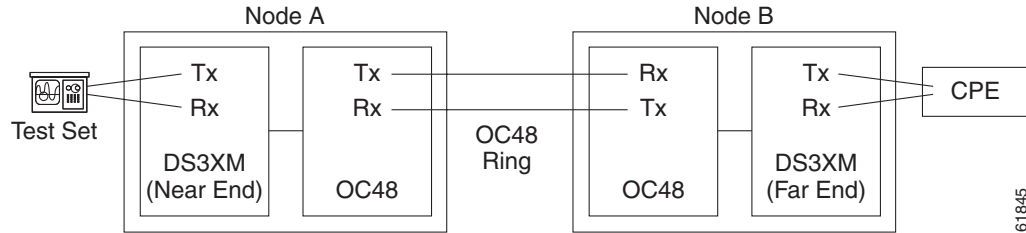
The DS3XM-6 card supports Far End Alarm and Control (FEAC) functions that are not available on basic DS-3 cards. Click the Maintenance tab at the DS3XM-6 card view to reveal the two additional function columns. [Figure 1-11](#) shows the DS3 subtab and the additional *Send Code* and *Inhibit FE Lbk* function columns.

Figure 1-11 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 1-12](#), 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 1-12 Diagram of FEAC



61845

1.3.1 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 transmuted into a DS-3 circuit.

1.3.2 FEAC Inhibit Loopback

The DS3XM-6 ports and transmuted 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.

1.3.3 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.

1.4 Identify Points of Failure on an OC-N Circuit Path

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

The example in this section tests an OC-N circuit on a three-node, bidirectional line switched ring (BLSR). Using a series of facility loopbacks and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of six network test procedures apply to this example 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 OC-N port
2. A terminal loopback on the source-node OC-N port
3. A facility loopback on the intermediate-node OC-N port
4. A terminal loopback on the intermediate-node OC-N port
5. A facility loopback on the destination-node OC-N port
6. A terminal loopback on the destination-node OC-N port

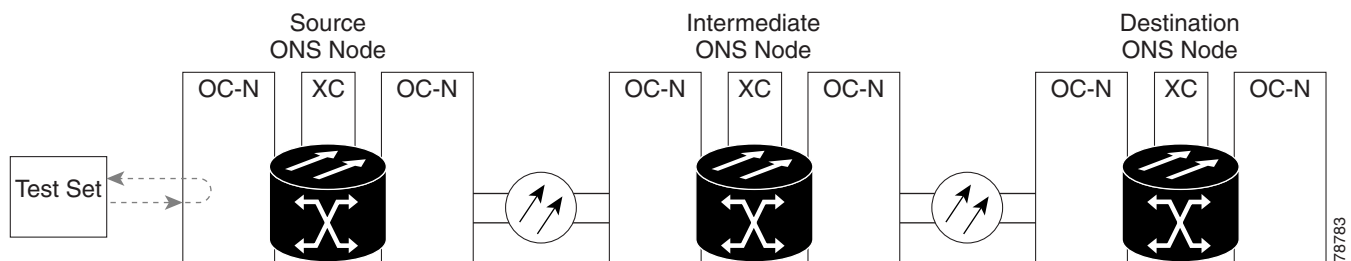
**Note**

All loopback tests require on-site personnel.

1.4.1 Perform a Facility Loopback on a Source-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the source node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-6 shows an example of a facility loopback on a circuit source OC-N port.

Figure 1-13 A facility loopback on a circuit source OC-N port

**Caution**

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

Procedure: Create the Facility Loopback on the Source OC-N Port

- Step 1** Connect an optical test set to the port you are testing.
- Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to 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:
- In node view, double-click the card where you will perform the loopback.
 - Click the **Maintenance > Loopback** tabs.
 - Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.
 - 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.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

- Step 3** Proceed to the [“Test the Facility Loopback Circuit”](#) section on page 1-24.

Procedure: Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback before testing the next segment of the network circuit path.
- Click the **Maintenance > Loopback** tabs.
 - Choose **None** from the Loopback Type column for the port being tested.
 - Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - Click the **Apply** button.
 - Click the **Yes** button in the Confirmation Dialog box.
- Proceed to the [“Perform a Terminal Loopback on a Source-Node OC-N Port”](#) section on page 1-25.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty OC-N card. Proceed to the [“Test the OC-N Card”](#) section on page 1-24.

Procedure: Test the OC-N Card

- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the faulty card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the facility loopback before testing the next segment of the network circuit path.

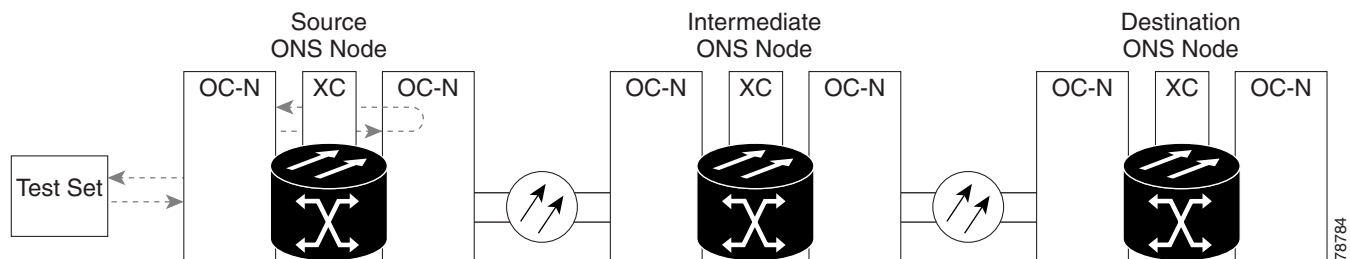
- a. Click the **Maintenance > Loopback** tabs.
- b. Choose **None** from the Loopback Type column for the port being tested.
- c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
- d. Click the **Apply** button.
- e. Click the **Yes** button in the Confirmation Dialog box.

Proceed to the [“Perform a Terminal Loopback on a Source-Node OC-N Port”](#) section on page 1-25.

1.4.2 Perform a Terminal Loopback on a Source-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the source node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. [Figure 1-8](#) shows an example of a terminal loopback on a destination OC-N port.

Figure 1-14 Terminal loopback on a source-node OC-N port



Caution

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

Procedure: Create the Terminal Loopback on a Source Node OC-N Port

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

- a. If you just completed the [“Perform a Facility Loopback on a Source-Node OC-N Port”](#) section on page 1-23, leave the optical test set hooked up to the OC-N port in the source node.

- b. If you are starting the current procedure without the optical test set hooked up to the OC-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to 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 “OCN1toOCN2”.
 - c. Set Circuit **Type** and **Size** to the normal preferences.
 - d. Leave the **Bidirectional** checkbox checked and click the **Next** button.
 - e. In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the source node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.



Note It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 4** Create the terminal loopback on the destination port being tested:
- a. In node view, double-click the card that requires the loopback, such as the destination OC-N card in the source node.
 - b. Click the **Maintenance > Loopback** tabs.
 - c. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
 - d. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - e. Click the **Apply** button.
 - f. Click the **Yes** button in the Confirmation Dialog box.
- Step 5** Proceed to the [“Test the Terminal Loopback Circuit” section on page 1-26](#).
-

Procedure: Test the Terminal Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback before testing the next segment of the network circuit path.
- a. Double-click the OC-N card in the source node with the terminal loopback.
 - b. Click the **Maintenance > Loopback** tabs.
 - c. Select **None** from the Loopback Type column for the port being tested.

- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “[Perform a Facility Loopback on an Intermediate-Node OC-N Port](#)” section on page 1-28.

Step 4 If the test set indicates a faulty circuit, the problem may be a faulty card.

Proceed to the “[Test the OC-N card](#)” section on page 1-27.

Procedure: Test the OC-N card

Step 1 Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the defective OC-N card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the terminal loopback before testing the next segment of the network circuit path.

- a. Double-click the OC-N card in the source node with the terminal loopback.
- b. Click the **Maintenance > Loopback** tabs.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.

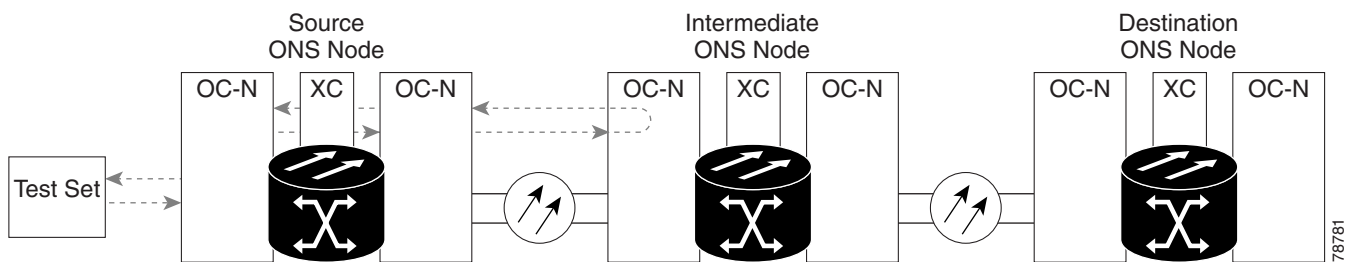
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “[Perform a Facility Loopback on an Intermediate-Node OC-N Port](#)” section on page 1-28.

1.4.3 Perform a Facility Loopback on an Intermediate-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the intermediate node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. [Figure 1-15](#) shows an example of a facility loopback on a intermediate node circuit source OC-N port.

Figure 1-15 Facility loopback on an intermediate-node OC-N port



Caution

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

Procedure: Create the Facility Loopback on an Intermediate-Node OC-N Port

- Step 1** Connect an optical test set to the port you are testing:
 - a. If you just completed the “[Perform a Terminal Loopback on a Source-Node OC-N Port](#)” section on page 1-25, leave the optical test set hooked up to the OC-N port in the source node.
 - b. If you are starting the current procedure without the optical test set hooked up to the OC-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to 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 facility 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 “OCN1toOCN3”.
 - c. Set Circuit **Type** and **Size** to the normal preferences.
 - d. Leave the **Bidirectional** checkbox checked and click the **Next** button.
 - e. In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.



Note It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 4** Create the facility loopback on the destination port being tested:
- a. Go to the node view of the intermediate node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down list in the Select Node box and click the **OK** button.
 - b. In node view, double-click the card that requires the loopback, such as the destination OC-N card in the intermediate node.
 - c. Click the **Maintenance > Loopback** tabs.
 - d. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
 - e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - f. Click the **Apply** button.
 - g. Click the **Yes** button in the Confirmation Dialog box.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

- Step 5** Proceed to the [“Test the Facility Loopback Circuit”](#) section on page 1-29.
-

Procedure: Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback before testing the next segment of the network circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - d. Click the **Apply** button.
 - e. Click the **Yes** button in the confirmation dialog box.
- Clear the facility loopback circuit before testing the next segment of the network circuit path.
- a. Click the **Circuits** tab.
 - b. Choose the loopback circuit being tested.
 - c. Click the **Delete** button.

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

Proceed to the “Perform a Terminal Loopback on an Intermediate-Node OC-N Port” section on page 1-31.

Step 4 If the test set indicates a faulty circuit, the problem may be a faulty OC-N card.

Proceed to the “Test the OC-N Card” section on page 1-30.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a known-good card. See Chapter 2, “Alarm Troubleshooting” for details.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the faulty card. See Chapter 2, “Alarm Troubleshooting” for details.

Clear the facility loopback before testing the next segment of the network circuit path.

- a. Click the **Maintenance > Loopback** tabs.
- b. Choose **None** from the Loopback Type column for the port being tested.
- c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
- d. Click the **Apply** button.
- e. Click the **Yes** button in the Confirmation Dialog box.

Clear the facility loopback circuit before testing the next segment of the network circuit path.

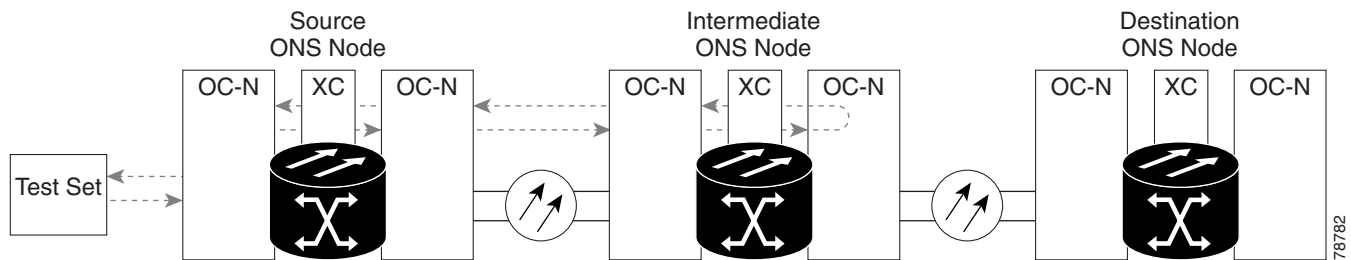
- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “Perform a Terminal Loopback on an Intermediate-Node OC-N Port” section on page 1-31.

1.4.4 Perform a Terminal Loopback on an Intermediate-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the intermediate node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. Figure 1-16 shows an example of a terminal loopback on an intermediate node destination OC-N port.

Figure 1-16 Terminal loopback on an intermediate-node OC-N port



Caution

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

Procedure: Create the Terminal Loopback on an Intermediate-Node OC-N Port

- Step 1** Connect an optical test set to the port you are testing:
 - a. If you just completed the [“Perform a Facility Loopback on an Intermediate-Node OC-N Port”](#) section on page 1-28, leave the optical test set hooked up to the OC-N port in the source node.
 - b. If you are starting the current procedure without the optical test set hooked up to the OC-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to 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 “OCN1toOCN4”.
 - c. Set **Circuit Type** and **Size** to the normal preferences.
 - d. Leave the **Bidirectional** checkbox checked and click the **Next** button.
 - e. In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.



Note It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 4** Create the terminal loopback on the destination port being tested:
- a. Go to the node view of the intermediate node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down list in the Select Node box and click the **OK** button.
 - b. In node view, double-click the card that requires the loopback, such as the destination OC-N card in the intermediate node.
 - c. Click the **Maintenance > Loopback** tabs.
 - d. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
 - e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
 - f. Click the **Apply** button.
 - g. Click the **Yes** button in the Confirmation Dialog box.
- Step 5** Proceed to the [“Test the Terminal Loopback Circuit”](#) section on page 1-32.

Procedure: Test the Terminal Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit.
- Clear the terminal loopback before testing the next segment of the network circuit path.
- a. Double-click the OC-N card in the intermediate node with the terminal loopback.
 - b. Click the **Maintenance > Loopback** tabs.
 - c. Select **None** from the Loopback Type column for the port being tested.
 - d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
 - e. Click the **Apply** button.
 - f. Click the **Yes** button in the Confirmation Dialog box.
- Clear the terminal loopback circuit before testing the next segment of the network circuit path.
- a. Click the **Circuits** tab.
 - b. Choose the loopback circuit being tested.
 - c. Click the **Delete** button.
 - d. Click the **Yes** button in the Delete Circuits box.
- Proceed to the [“Perform a Facility Loopback on a Destination-Node OC-N Port”](#) section on page 1-33.

- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty card. Proceed to the “[Test the OC-N card](#)” section on page 1-33.
-

Procedure: Test the OC-N card

- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details. Resend test traffic on the loopback circuit with a known-good card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- Step 2** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Replace the defective OC-N card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the terminal loopback before testing the next segment of the network circuit path.

- a. Double-click the OC-N card in the source node with the terminal loopback.
- b. Click the **Maintenance > Loopback** tabs.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

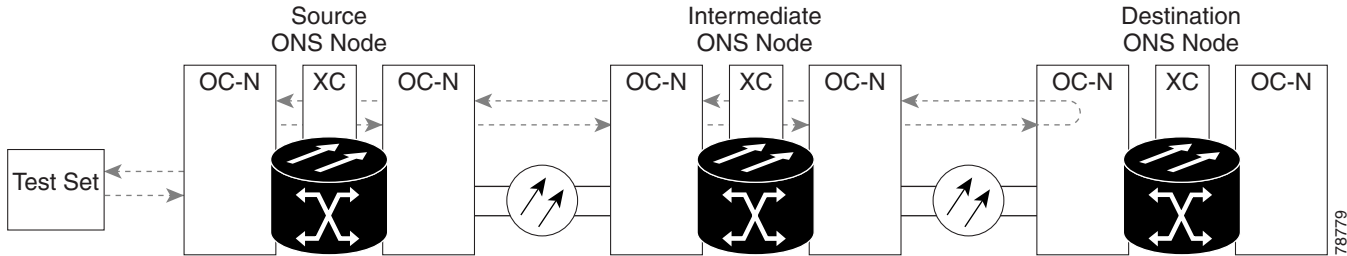
- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the “[Perform a Facility Loopback on a Destination-Node OC-N Port](#)” section on page 1-33.

1.4.5 Perform a Facility Loopback on a Destination-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the destination node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. [Figure 1-17](#) shows an example of a facility loopback on a destination node circuit source OC-N port.

Figure 1-17 Facility loopback on a destination-node OC-N port

**Caution**

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

Procedure: Create the Facility Loopback on a Destination-Node OC-N Port

- Step 1** Connect an optical test set to the port you are testing:
- If you just completed the [“Perform a Terminal Loopback on an Intermediate-Node OC-N Port”](#) section on page 1-31, leave the optical test set hooked up to the OC-N port in the source node.
 - If you are starting the current procedure without the optical test set hooked up to the OC-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.
 - Adjust the test set accordingly.
- Step 2** Use CTC to set up the facility loopback circuit on the port being tested.
- Click the **Circuits** tab and click the **Create** button.
 - Give the circuit an easily identifiable name, such as “OCN1toOCN5”.
 - Set Circuit **Type** and **Size** to the normal preferences.
 - Leave the **Bidirectional** checkbox checked and click the **Next** button.
 - In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

**Note**

It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 4** Create the facility loopback on the destination port being tested:
- Go to the node view of the destination node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down list in the Select Node box and click the **OK** button.
 - In node view, double-click the card that requires the loopback, such as the destination OC-N card in the destination node.

- c. Click the **Maintenance > Loopback** tabs.
- d. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
- e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
- f. Click the **Apply** button.
- g. Click the **Yes** button in the Confirmation Dialog box.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

Step 5 Proceed to the [“Test the Facility Loopback Circuit”](#) section on page 1-29.

Procedure: Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback before testing the next segment of the network circuit path.
- a. Click the **Maintenance > Loopback** tabs.
 - b. Choose **None** from the Loopback Type column for the port being tested.
 - c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
 - d. Click the **Apply** button.
 - e. Click the **Yes** button in the confirmation dialog box.
- Clear the facility loopback circuit before testing the next segment of the network circuit path.
- a. Click the **Circuits** tab.
 - b. Choose the loopback circuit being tested.
 - c. Click the **Delete** button.
 - d. Click the **Yes** button in the Delete Circuits box.
- Proceed to the [“Perform a Terminal Loopback on a Destination-Node OC-N Port”](#) section on page 1-36.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty OC-N card. Proceed to the [“Test the OC-N Card”](#) section on page 1-30.

Procedure: Test the OC-N Card

- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the faulty card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the facility loopback before testing the next segment of the network circuit path.

- a. Click the **Maintenance > Loopback** tabs.
- b. Choose **None** from the Loopback Type column for the port being tested.
- c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.
- d. Click the **Apply** button.
- e. Click the **Yes** button in the Confirmation Dialog box.

Clear the facility loopback circuit before testing the next segment of the network circuit path.

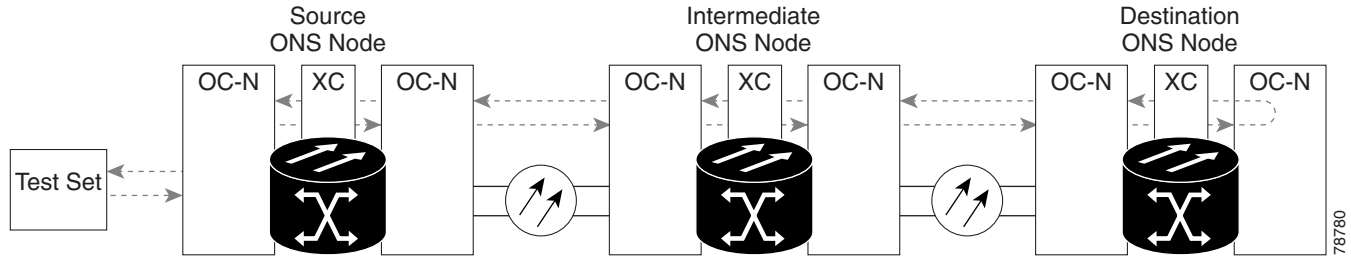
- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

Proceed to the [“Perform a Terminal Loopback on a Destination-Node OC-N Port”](#) section on page 1-36.

1.4.6 Perform a Terminal Loopback on a Destination-Node OC-N Port


The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the destination node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. [Figure 1-18](#) shows an example of a terminal loopback on an intermediate node destination OC-N port.

Figure 1-18 Terminal loopback on a destination-node OC-N port

**Caution**

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

Procedure: Create the Terminal Loopback on a Destination-Node OC-N Port

- Step 1** Connect an optical test set to the port you are testing:
- If you just completed the “[Perform a Facility Loopback on a Destination-Node OC-N Port](#)” section on page 1-33, leave the optical test set hooked up to the OC-N port in the source node.
 - If you are starting the current procedure without the optical test set hooked up to the OC-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.
 - Adjust the test set accordingly.
- Step 2** Use CTC to set up the terminal loopback circuit on the port being tested.
- Click the **Circuits** tab and click the **Create** button.
 - Give the circuit an easily identifiable name, such as “OCN1toOCN6”.
 - Set Circuit **Type** and **Size** to the normal preferences.
 - Leave the **Bidirectional** checkbox checked and click the **Next** button.
 - In the Circuit Source dialog box, fill in the same **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
 - In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.
- Step 3** Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.
-  **Note** It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.
- Step 4** Create the terminal loopback on the destination port being tested:
- Go to the node view of the destination node:
 - Choose **View > Go To Other Node** from the menu bar.
 - Choose the node from the pull-down list in the Select Node box and click the **OK** button.
 - In node view, double-click the card that requires the loopback, such as the destination OC-N card in the destination node.

- c. Click the **Maintenance > Loopback** tabs.
- d. Select OOS_MT from the State column. If this is a multiport card, select the row appropriate for the desired port.
- e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
- f. Click the **Apply** button.
- g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the “[Test the Terminal Loopback Circuit](#)” section on page 1-38.

Procedure: Test the Terminal Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback before testing the next segment of the network circuit path.
- a. Double-click the OC-N card in the intermediate node with the terminal loopback.
 - b. Click the **Maintenance > Loopback** tabs.
 - c. Select **None** from the Loopback Type column for the port being tested.
 - d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
 - e. Click the **Apply** button.
 - f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

The entire OC-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 card. Proceed to the “[Test the OC-N Card](#)” section on page 1-38.
-

Procedure: Test the OC-N Card

- Step 1** Replace the suspect card with a known-good card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

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

Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-877-323-7368 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL:

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

Replace the defective OC-N card. See [Chapter 2, “Alarm Troubleshooting”](#) for details.

Clear the terminal loopback before testing the next segment of the network circuit path.

- a. Double-click the OC-N card in the source node with the terminal loopback.
- b. Click the **Maintenance > Loopback** tabs.
- c. Select **None** from the Loopback Type column for the port being tested.
- d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.
- e. Click the **Apply** button.
- f. Click the **Yes** button in the Confirmation Dialog box.

Clear the terminal loopback circuit before testing the next segment of the network circuit path.

- a. Click the **Circuits** tab.
- b. Choose the loopback circuit being tested.
- c. Click the **Delete** button.
- d. Click the **Yes** button in the Delete Circuits box.

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

1.5 Restoring the Database and Default Settings

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

1.5.1 Restore the Node Database

Symptom: One or more node(s) are not functioning properly or have incorrect data.

[Table 1-1](#) describes the potential cause(s) of the symptom and the solution(s).

Table 1-1 Restore the Node Database

Possible Problem	Solution
Incorrect or corrupted node database.	Perform a Restore the Database procedure. Refer to the “Restore the Database” section on page 1-40.

Procedure: Restore the Database



Note

The following parameters are not backed up and restored: node name, IP address, mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new renamed node. Cisco recommends keeping a record of the old and new node names.



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 re convergence. The CARLOSS alarm will appear and clear during this period.



Caution

If you are restoring the database on multiple nodes, wait until the TCC+ reboot has completed on each node before proceeding to the next node.

Step 1

Log into the node where you will restore the database.

- a. On the PC connected to the ONS 15454, start Netscape or Internet Explorer.
- b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address.
A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages display while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box displays.
- c. In the Login dialog box, type a user name and password (both are case sensitive) and click the **Login** button. The CTC node view window will appear.

Step 2

Ensure that there are no ring or span (four-fiber only) switch events; for example, ring-switch east or west, and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve Conditions** to view a list of conditions.

Step 3

If there are switch events that need to be cleared, in node (default) view, click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

- a. If there is a switch event (not caused by a line failure), clear the switch by choosing **CLEAR** from the pull-down menu and click **Apply**.
- b. If there is a switch event caused by the Wait to Restore (WTR) condition, choose **LOCKOUT SPAN** from the pull-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the pull-down menu and click **Apply**.

Step 4

In node view, click the **Maintenance > Database** tabs.

Step 5

Click **Restore**.

Step 6 Locate the database file stored on the workstation's hard drive or on network storage.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears.



Caution Opening a restore file from another node or from an earlier backup may affect traffic on the login node.

Step 9 Click **Yes**.

The Restore Database dialog box monitors the file transfer.

Step 10 Wait for the file to complete the transfer to the TCC+ card.

Step 11 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears. Wait for the node to reconnect.

Step 12 If you cleared a switch in [Step 3](#), reapply the switch as needed.

1.5.2 Restore the Node to Factory Configuration

Symptom A node has both TCC+ cards in standby state, and you are unable reset the TCC+ cards to make the node functional.

[Table 1-2](#) describes the potential cause(s) of the symptom and the solution(s).

Table 1-2 *Restore the Node to Factory Configuration*

Possible Problem	Solution
Failure of both TCC+ cards in the node.	This procedure describes how to restore the node to factory configuration using the RE-INIT.jar JAVA file, which is referred to as the reinitialization tool in this documentation. Use this tool to upload the software package and/or restore the database after it has been backed up. You will need the CD containing the latest software, the node's NE defaults, and the recovery tool. Restore the node to factory configuration. Refer to the " DLP-244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) " section on page 1-42 or the " DLP-245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX) " section on page 1-43.
Replacement of both TCC+ cards at the same time.	



Caution If you are restoring the database on multiple nodes, wait until the TCC+ cards have rebooted on each node before proceeding to the next node.



Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you only use the Search Path field. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

**Note**

If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-19 on page 1-42).

**Note**

The following parameters are not backed up and restored: node name, IP address, mask and gateway, and IOP port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Procedure: DLP-244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

**Note**

The TCC+ cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

- Step 1** Insert the system software CD containing the reinit tool (Figure 1-19) into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.
- Step 2** To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.
- Step 3** On the CD drive, go to the **CISCO15454** folder and set the Files of Type drop-down menu to **All Files**.
- Step 4** Select the **RE-INIT.jar** file and click **Open** to open the reinit tool (Figure 1-19).

Figure 1-19 Reinitialization tool in Windows

- Step 5** If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.
- Step 6** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-19).
- Step 7** Verify that the Re-Init Database, Upload Package, and Confirm checkboxes are checked. If one is not checked, click the checkbox.
- Step 8** In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

**Caution**

Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

**Caution**

Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

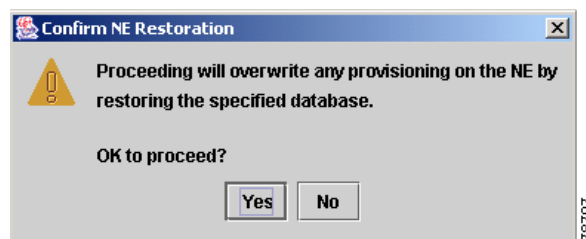
- Step 9** Click **Go**.
- Step 10** A confirmation dialog box opens (Figure 1-20). Click **Yes**.
- Step 11** The status bar at the bottom of the screen will display Complete when the node has activated the software and uploaded the database.

**Note**

The Complete message only indicates that the TCC+ successfully uploaded the database, not that the database restore was successful. The TCC+ will then try to restore the database after it reboots.

- Step 12** If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC+ or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15454 Procedures Guide*.
- Step 13** Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedures Guide* for information on setting the node name, IP address, mask and gateway, and IIO port.

Figure 1-20 Confirm NE Restoration



Procedure: DLP-245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

**Note**

JRE 1.03_02 must also be installed on the computer you will use to perform this procedure.

**Note**

The TCC+ cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

- Step 1** Insert the system software CD containing the reinit tool, software, and defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.
- Step 2** To find the recovery tool file, go to the CISCO15454 directory on the CD (usually `/cdrom/cdrom0/CISCO15454`).
- Step 3** If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinit tool (Figure 1-21). If you are working with a command line interface, run `java -jar RE-INIT.jar`.

Figure 1-21 The reinitialization tool in UNIX

- Step 4** If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.
- Step 5** Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-21).
- Step 6** Verify that the Re-Init Database, Upload Package, and Confirm checkboxes are checked. If any are not checked, click that checkbox.
- Step 7** In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

**Caution**

Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

**Caution**

Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

- Step 8** Click **Go**.
- Step 9** A confirmation dialog box opens (Figure 1-20 on page 1-43). Click **Yes**.

- Step 10** The status bar at the bottom of the screen will display Complete when the node has activated the software and uploaded the database.



Note The Complete message only indicates that the TCC+ successfully uploaded the database, not that the database restore was successful. The TCC+ will then try to restore the database after it reboots.

- Step 11** If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC+ or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15454 Procedures Guide*.
- Step 12** Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedures Guide* for information on setting the node name, IP address, mask and gateway, and IOP port.

1.6 PC Connectivity Troubleshooting

This section contains troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.6.1 Unable to Verify the IP Configuration of your PC

Symptom When connecting your PC to the ONS 15454, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

[Table 1-3](#) describes the potential cause(s) of the symptom and the solution(s).

Table 1-3 Unable to Verify the IP Configuration of your PC

Possible Problem	Solution
The IP address was typed incorrectly.	Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. Refer to the “Verify the IP Configuration of your PC” section on page 1-45 .
The IP configuration of your PC is not properly set.	To verify the IP configuration of your PC, refer to the “Verify the IP Configuration of your PC” section on page 1-45 . If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Procedure: Verify the IP Configuration of your PC

- Step 1** Open a DOS command window by selecting **Start > Run** from the Start menu.
- Step 2** In the Run window open field, type **command** and then click the **OK** button. The DOS command window will appear.

Step 3 At the prompt in the DOS window, type one of the following appropriate commands:

- For Windows 98, NT, and 2000, type **ipconfig** and press the **Enter** key.
- For Windows 95, type **winipcfg** and press the **Enter** key.

The Windows IP configuration information will be displayed, including the IP address, Subnet Mask, and the Default Gateway.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information previously displayed.

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

If the DOS window displays multiple (usually four) replies, the IP configuration is working properly.

If you do not receive a reply, your IP configuration may not be properly set. Contact your Network Administrator for instructions to correct the IP configuration of your PC.

1.6.2 Browser Login Does Not Launch Java

Symptom The message “Loading Java Applet” does not appear and the JRE does not launch during the initial login.

Table 1-4 describes the potential cause(s) of the symptom and the solution(s).

Table 1-4 *Browser Login Does Not Launch Java*

Possible Problem	Solution
The PC operating system and browser are not properly configured.	Reconfigure the PC operating system java plug-in control panel and the browser settings. See the “Reconfigure the PC Operating System Java Plug-in Control Panel” section on page 1-46 and the “Reconfigure the Browser” section on page 1-47.

Procedure: Reconfigure the PC Operating System Java Plug-in Control Panel

Step 1 From the Windows start menu, click **Settings > Control Panel**.

Step 2 If **Java Plug-in Control Panel** does not appear, the JRE may not be installed on your PC.

- a. Run the Cisco ONS 15454 software CD.
- b. Open the [CD drive]:\Windows\JRE folder.
- c. Double-click the j2re-1_3_1_02-win icon to run the JRE installation wizard.
- d. Follow the JRE installation wizard steps.

Step 3 From the Windows start menu, click **Settings > Control Panel**.

Step 4 In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.3.1_02** icon.

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

Step 6 From the Java Run Time Environment menu, select **JRE 1.3 in C:\ProgramFiles\JavaSoft\JRE\1.3.1_02**.

- Step 7** Click the **Apply** button.
- Step 8** Close the Java Plug-in Control Panel window.
-

Procedure: Reconfigure the Browser

- Step 1** From the Start Menu, launch your browser application.
- Step 2** If you are using Netscape Navigator:
- On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.
 - In the Preferences window, click the **Advanced > Proxies** categories.
 - In the Proxies window, click the **Direct connection to the Internet** checkbox and click the **OK** button.
 - On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.
 - In the Preferences window, click the **Advanced > Cache** categories.
 - Confirm that the Disk Cache Folder field shows one of the following paths:
 - For Windows 95/98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**
 - For Windows NT/2000, **C:\ProgramFiles\Netscape\<username>\Communicator\cache**.
 - If the Disk Cache Folder field is not correct, click the **Choose Folder** button.
 - Navigate to the file listed in **f**. and click the **OK** button.
 - Click the **OK** button on the Preferences window and exit the browser.
- Step 3** If you are using Internet Explorer:
- On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.
 - In the Internet Options window, click the **Advanced** tab.
 - In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.3.1_02 for <applet> (requires restart)** checkbox.
 - Click the **OK** button in the Internet Options window and exit the browser.
- Step 4** Temporarily disable any virus-scanning software on the computer. See the [“Browser Stalls When Downloading CTC JAR Files From TCC+”](#) section on page 1-50.
- Step 5** Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.
- Step 6** Restart the browser and logon to the ONS 15454.
-

1.6.3 Unable to Verify the NIC Connection on your PC

Symptom When connecting your PC to the ONS 15454, you are unable to verify the NIC connection is working properly because the link LED is not illuminated or flashing.

[Table 1-5](#) describes the potential cause(s) of the symptom and the solution(s).

Table 1-5 Unable to Verify the NIC Connection on your PC

Possible Problem	Solution
The Category 5 cable is not plugged in properly.	Confirm both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.
The Category 5 cable is damaged.	Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending
Incorrect type of Category 5 cable is being used.	If connecting an ONS 15454 directly to your laptop/PC or a router, use a straight-through CAT-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of Category 5 cables, see the “Crimp Replacement LAN Cables” section on page 1-75.
The NIC is improperly inserted or installed.	If you are using a PCMCIA based NIC, remove and re-insert the NIC to make sure the NIC is fully inserted. If the NIC is built into the laptop/PC, verify that the NIC is not faulty.
The NIC is faulty.	Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting a to the network (or any other node), then the NIC may be faulty and needs to be replaced.

1.6.4 Verify PC Connection to the ONS 15454 (ping)

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

Table 1-6 describes the potential cause(s) of the symptom and the solution(s).

Table 1-6 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 1-48.

Procedure: 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.

1.7 CTC Operation Troubleshooting

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

1.7.1 Unable to Change Node View to Network View

Symptom When activating a large, multi node BLSR from Software Release 3.2 to Software Release 3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an “Exception occurred during event dispatching: java.lang.OutOfMemoryError” in the java window.

Table 1-7 describes the potential cause(s) of the symptom and the solution(s).

Table 1-7 Browser Stalls When Downloading Files From TCC+

Possible Problem	Solution
The large, multi node BLSR requires more memory for the GUI environment variables.	<p>Reset the system or user CTC_HEAP environment variable to increase the memory limits.</p> <p>See the “Reset the CTC_HEAP Environment Variable for Windows” section on page 1-49 or the “Reset the CTC_HEAP Environment Variable for Solaris” section on page 1-50 to enable the CTC_HEAP variable change.</p> <p>Note This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.</p>

Procedure: 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.

Procedure: 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.

---

## 1.7.2 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 1-8](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-8** *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 <a href="#">“Disable the VirusScan Download Scan”</a> section on page 1-50. |

---

## Procedure: Disable the VirusScan Download Scan

- Step 1** From the Windows start menu, choose **Programs > Network Associates > VirusScan Console**.
- Step 2** Double-click the **VShield** icon listed in the VirusScan Console dialog box.
- Step 3** Click the **Configure** button on the lower part of the Task Properties window.

- Step 4** Click the **Download Scan** icon on the left of the System Scan Properties dialog box.
  - Step 5** Uncheck the **Enable Internet download scanning** checkbox.
  - Step 6** Click **Yes** when the warning message appears.
  - Step 7** Click **OK** on the System Scan Properties dialog box.
  - Step 8** Click **OK** on the Task Properties window.
  - Step 9** Close the McAfee VirusScan window.
- 

## 1.7.3 CTC Does Not Launch

**Symptom** CTC does not launch, usually an error message appears before the login screen displays.

[Table 1-9](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-9 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 <a href="#">“Redirect the Netscape Cache to a Valid Directory”</a> section on page 1-51. |

### Procedure: Redirect the Netscape Cache to a Valid Directory

- Step 1** Launch Netscape.
- Step 2** Display the **Edit** menu.
- Step 3** Choose **Preferences**.
- Step 4** Under the Category column on the left-hand side, go to **Advanced** and choose the **Cache** tab.
- Step 5** Change your disk cache folder to point to the cache file location.

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

---

## 1.7.4 Sluggish CTC Operation or Login Problems

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

[Table 1-10](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-10 Sluggish CTC Operation or Login Problems**

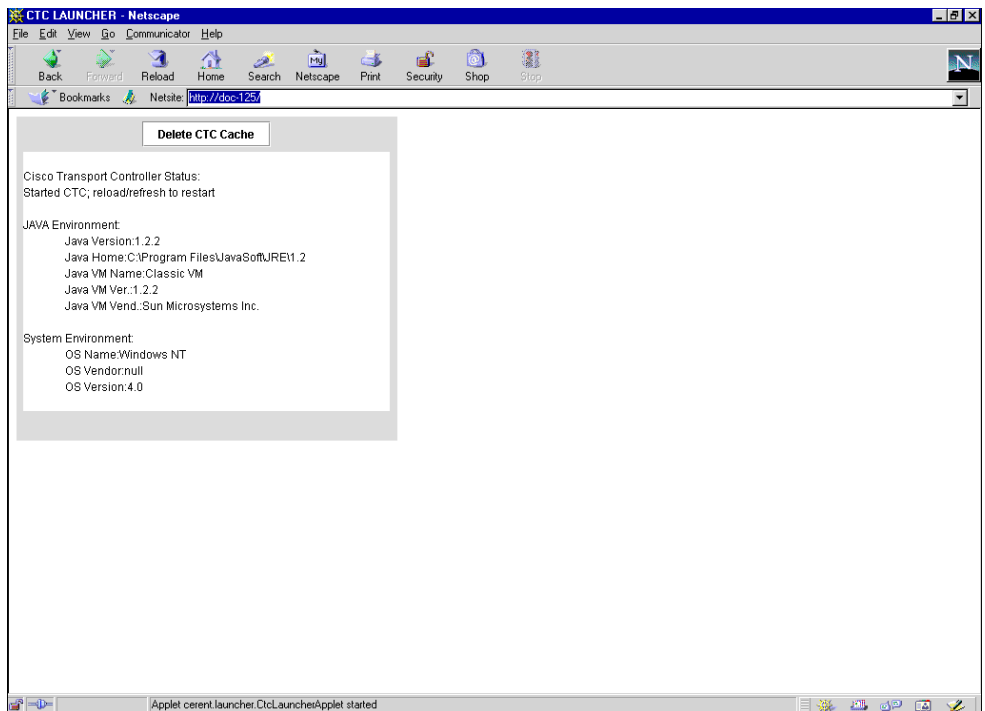
| Possible Problem                                                | Solution                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 “ <a href="#">Delete the CTC Cache File Automatically</a> ” section on page 1-52 or the “ <a href="#">Delete the CTC Cache File Manually</a> ” section on page 1-53. |

## Procedure: 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 1-22](#) 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 1-22 Deleting the CTC cache**

## Procedure: Delete the CTC Cache File Manually

- 
- Step 1** To delete the jar files manually, from the Windows Start menu choose **Search > For Files or Folders**.
- Step 2** Enter \*.jar in the Search for files or folders named field on the Search Results dialog box and click **Search Now**.
- Step 3** Click the **Modified** column on the Search Results dialog box to find the jar files that match the date when you downloaded the files from the TCC+. 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.
- 

## 1.7.5 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 1-11](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-11 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 <a href="#">“Different CTC Releases Do Not Recognize Each Other”</a> section on page 1-56. |
| A username/password mismatch.                      | Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the <a href="#">“Username or Password Do Not Match”</a> section on page 1-56.              |
| No IP connectivity between nodes.                  | Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the <a href="#">“Ethernet Connections”</a> section on page 1-59.                              |
| A lost DCC connection.                             | Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the <a href="#">“EOC”</a> section on page 2-44.                                         |

## 1.7.6 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 1-12](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-12 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. | <ol style="list-style-type: none"> <li>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 <i>Cisco ONS 15454 Procedure Guide</i> for instructions).</li> <li>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 <a href="#">“Manually Edit the java.policy File”</a> section on page 1-54.</li> </ol> |

## Procedure: Manually Edit the java.policy File

**Step 1** Search your computer for this file and open it with a text editor (Notepad or Wordpad).

**Step 2** Verify that the end of this file has the following lines:

```
// Insert this into the system-wide or a per-user java.policy file.
// DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!

grant codeBase "http://*/fs/LAUNCHER.jar" {
permission java.security.AllPermission;
};
```

**Step 3** If these five lines are not in the file, enter them manually.

**Step 4** Save the file and restart Netscape.

CTC should now start correctly.

**Step 5** If the error message is still reported, save the java.policy file as (**.java.policy**). On Win95/98/2000 PCs, save the file to the C:\Windows folder. On WinNT4.0 PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

## 1.7.7 Java Runtime Environment Incompatible

**Symptom** The CTC application will not run properly.

[Table 1-13](#) describes the potential cause(s) of the symptom and the solution(s).



**Table 1-13 Java Runtime Environment Incompatible**

| Possible Problem                                 | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Do not have the compatible Java 2 JRE installed. | <p>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.</p> <p>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 <a href="#">“Launch CTC to Correct the Core Version Build”</a> section on page 1-55.</p> <p>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. <a href="#">Table 1-14</a> shows JRE compatibility with ONS 15454 software releases.</p> |

**Table 1-14 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                |
| ONS 15454 Release 3.3               | Yes                  | Yes                |

## Procedure: 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.

---

## 1.7.8 Different CTC Releases Do Not Recognize Each Other

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

[Table 1-15](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-15 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. | <p>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.</p> <p><b>Note</b> 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.</p> <p>See the <a href="#">“Launch CTC to Correct the Core Version Build”</a> section on <a href="#">page 1-56</a>.</p> |

### Procedure: 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.

---

## 1.7.9 Username or Password Do Not Match

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

[Table 1-16](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-16 Username or Password Do Not Match**

| Possible Problem                                                                  | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The username or password entered do not match the information stored in the TCC+. | <p>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.</p> <p>For initial logon to the ONS 15454, type the <i>CISCO15</i> user name in capital letters and click <b>Login</b> (no password is required). If you are using a CTC software release prior to 3.0 and <i>CISCO15</i> does not work, type <i>cerent454</i> for the user name.</p> <p>See the “Verify Correct Username and Password” section on page 1-57.</p> |

### Procedure: Verify Correct Username and Password

- 
- Step 1** Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.
- Step 2** Contact your system administrator to verify the username and password.
- Step 3** Call Cisco TAC at 1-877-323-7368 to have them enter your system and create a new user name and password.
- 

## 1.7.10 No IP Connectivity Exists Between Nodes

**Symptom** The nodes have a grey icon and is usually accompanied by alarms.

[Table 1-17](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-17 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 <a href="#">page 1-59</a> . |

## 1.7.11 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 1-18](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-18 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 2-44. |

## 1.7.12 “Path in Use” Error When Creating a Circuit

**Symptom** While creating a circuit, you get a “Path in Use” error that prevents you from completing the circuit creation.

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

**Table 1-19 “Path in Use” error when creating a circuit**

| Possible Problem                                                                  | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Another user has already selected the same source port to create another circuit. | <p>CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning will get use of the port. The other user will get the “Path in Use” error.</p> <p>Cancel the circuit creation and start over, or click the <b>Back</b> button until you return to the initial circuit creation screen. The source port that was previously selected will no longer appear in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.</p> |

## 1.7.13 Calculate and Design IP Subnets

**Symptom** You cannot calculate or design IP subnets on the ONS 15454.

Table 1-20 describes the potential cause(s) of the symptom and the solution(s).

**Table 1-20 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 <a href="http://www.cisco.com/techtools/ip_addr.html">http://www.cisco.com/techtools/ip_addr.html</a> . For information about ONS 15454 IP capability, refer to the <i>Cisco ONS 15454 Reference Manual</i> . |

## 1.7.14 Ethernet Connections

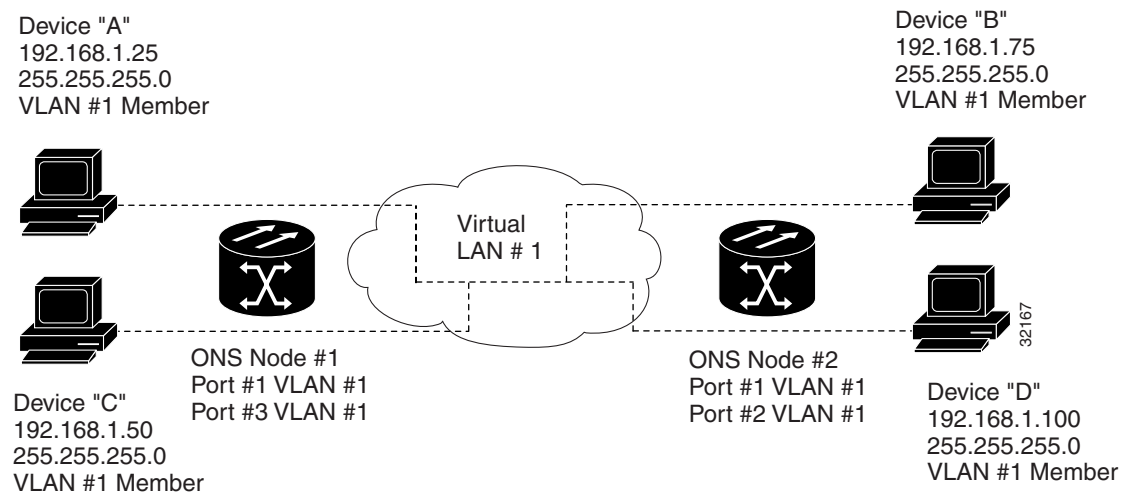
**Symptom** Ethernet connections appear to be broken or are not working properly.

[Table 1-21](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-21 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 <a href="#">Figure 1-23</a> when consulting the steps in the “ <a href="#">Verify Ethernet Connections</a> ” section on page 1-59. |
| Incorrect connections.         |                                                                                                                                                                                                                                     |

**Figure 1-23 Ethernet connectivity reference**



### Procedure: Verify Ethernet Connections

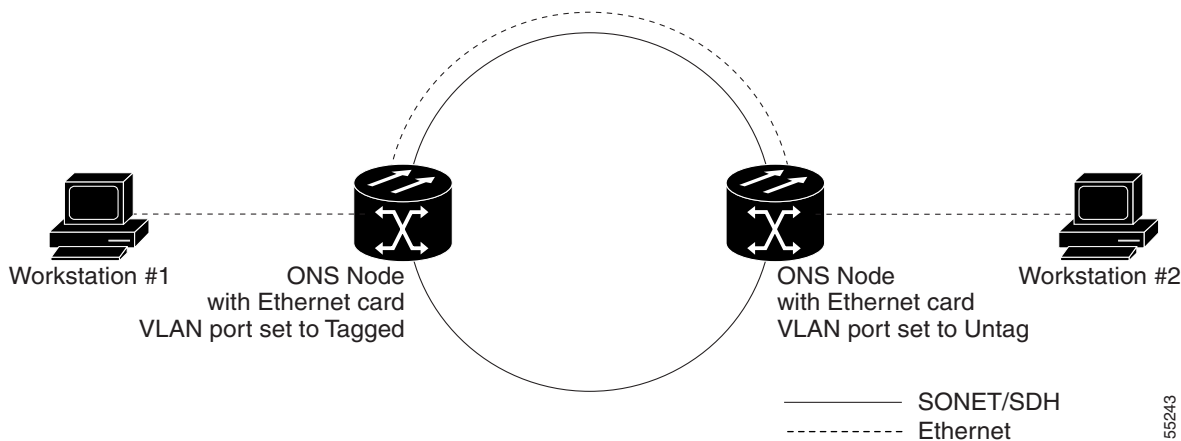
- Step 1** Check for SONET alarms on the STS-N that carries the VLAN #1 Ethernet circuit. Clear any alarms by looking them up in [Chapter 2, “Alarm Troubleshooting.”](#)
- Step 2** Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in [Chapter 2, “Alarm Troubleshooting.”](#)
- 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 1-80.
- Step 6** Verify connectivity between device A and device C by pinging between these locally attached devices (see the “[Verify PC Connection to the ONS 15454 \(ping\)](#)” section on page 1-48). 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.

## 1.7.15 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 1-24](#)). They may also see a higher than normal runt packets count at the network device attached to the Untag port.

**Figure 1-24** A VLAN with Ethernet ports at Tagged and Untag



[Table 1-22](#) describes the potential cause(s) of the symptom and the solution(s).

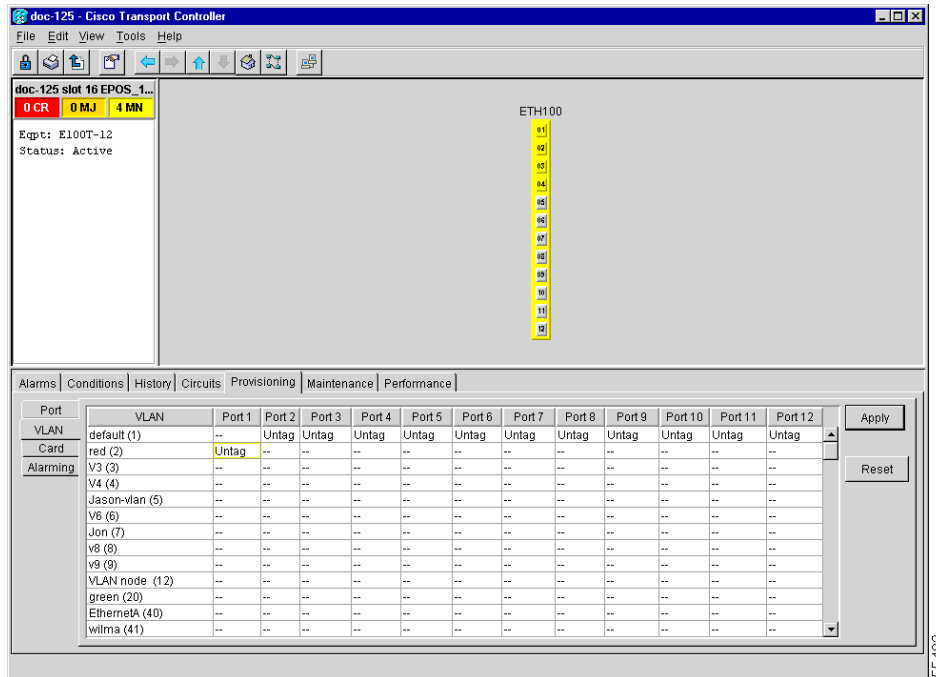
**Table 1-22 Verify PC connection to ONS 15454 (ping)**

| 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.        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Procedure: Change VLAN Port Tag and Untagged Settings

- 
- Step 1** Display the CTC card view for the Ethernet card involved in the problem VLAN.
- Step 2** Click the **Provisioning > VLAN** tabs ([Figure 1-25](#)).

Figure 1-25 Configuring VLAN membership for individual Ethernet ports



- Step 3** If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.
- Step 4** At the VLAN port set to **Untag**, click the port and choose **Tagged**.



**Note** The attached external devices must recognize IEEE 802.1Q VLANs.

- Step 5** After each port is in the appropriate VLAN, click **Apply**.

## 1.7.16 Cross-Connect Card Oscillator Fails

**Symptom:** The XC, XCVT, or XC10G card can be affected by this problem. It is indicated by a CTNEQPT-PBPROT or CTNEQPT-PBWORK condition raised against all I/O cards in the node. The following conditions might also be raised on the node:

- SWMTXMOD against one or both cross-connect cards
- 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 1-23 describes the potential cause(s) of the symptom and the solution(s).



Table 1-23 Cross-Connect Card Oscillator Fails

| Possible Problem                                    | Solution                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The XC, XCVT, or XC10G card has oscillator failure. | <ol style="list-style-type: none"> <li>1. If the Slot 8 cross-connect card is active, see the <a href="#">“Resolve the XC Oscillator Failure When Slot 8 XC Card is Active”</a> section on page 1-63.</li> <li>2. If the Slot 10 cross-connect card is active, see the <a href="#">“Resolve the XC Oscillator Failure When Slot 10 XC Card is Active”</a> section on page 1-63.</li> </ol> |

## Procedure: Resolve the XC Oscillator Failure When Slot 8 XC Card is Active

- 
- Step 1** If the CTNEQPT-PBPROT condition is reported against all I/O cards in the node and the Slot 8 cross-connect card is active, right-click the Slot 10 cross-connect card.
- Step 2** Choose **Reset Card**, then click **OK**. (Slot 8 remains active and Slot 10 remains standby.)
- Step 3** If the alarm remains, reseal the Slot 10 card.
- Step 4** If CTNEQPT-PBPROT does not clear, replace the Slot 10 cross-connect card with a spare card.
- Step 5** If CTNEQPT-PBPROT does not clear, replace the spare card placed in Slot 10 with the original cross-connect card.
- Step 6** Right-click the Slot 8 card and choose **Reset Card**.
- Step 7** Click **OK** to activate the Slot 10 card and place the Slot 8 card in standby.
- Step 8** If you then see the CTNEQPT-PBWORK condition raised against all I/O cards in the node, verify that CTNEQPT-PBPROT has cleared on all I/O cards. Seeing CTNEQPT-PBWORK on the cards indicates that Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. Otherwise, go to [Step 9](#).
- a. Replace the Slot 8 cross-connect card with a spare card. (Slot 8 remains standby.)
  - b. Reseat the Slot 10 cross-connect card to activate the Slot 8 card and make Slot 10 standby.
  - c. Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.
- Step 9** If you see CTNEQPT-PBPROT reported against all I/O cards in the node, this indicates that the Slot 10 card has a bad oscillator. If so, complete the following steps:
- a. Replace the Slot 10 cross-connect card with a spare card. (The Slot 8 card is now active.)
  - b. Reseat the Slot 8 cross-connect card to make Slot 10 active.
  - c. Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.
- 

## Procedure: Resolve the XC Oscillator Failure When Slot 10 XC Card is Active

- 
- Step 1** If the CTNEQPT-PBWORK condition is reported against all I/O cards in the node and the Slot 10 card is active, right-click the Slot 8 cross-connect card.
- Step 2** Choose **Reset Card** and click **OK**. (Slot 10 remains active and Slot 8 remains standby.)
- Step 3** If the CTNEQPT-PBWORK condition does not clear, reseal the Slot 8 cross-connect card.
- Step 4** If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.

- Step 5** If the condition does not clear, replace the spare card placed in Slot 8 with the original cross-connect card.
- Step 6** Right-click the Slot 10 cross-connect card.
- Step 7** Choose **Reset Card** and click **OK**. The Slot 8 cross-connect card becomes active and Slot 10 becomes standby.
- Step 8** If you have switched the Slot 8 card to active and continue to see CTNEQPT-PBWORK reported against all I/O cards in the node, this indicates the Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. If not, go to [Step 9](#).
- Replace the Slot 8 cross-connect card with a spare card. (The Slot 10 card is made active.)
  - Reseat the Slot 10 cross-connect card to make Slot 8 active.
  - Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.
- Step 9** If you then see the CTNEQPT-PBPROT condition raised against all I/O cards, verify that CTNEQPT-PBWORK has cleared on the I/O cards. This indicates that Slot 10 has a bad oscillator. If so, complete the following substeps:
- Replace the Slot 10 cross-connect card with a spare card. (Slot 10 remains standby.)
  - Reseat the Slot 8 cross-connect card to activate the Slot 10 card and make Slot 8 standby.
  - Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.
- 

## 1.8 Circuits and Timing

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

### 1.8.1 Circuit Transitions to Partial State

**Symptom** An automatic or manual transition of a circuit from one state to another state results in one of the following partial state conditions:

- **OOS\_PARTIAL** At least one of the connections in the circuit is in **OOS** state and at least one other connection in the circuit is in **IS**, **OOS\_MT**, or **OOS\_AINS** state.
- **OOS\_MT\_PARTIAL** At least one connection in the circuit is in **OOS\_MT** state and at least one other connection in the circuit is in **IS**, **OOS\_MT**, or **OOS\_AINS** state.
- **OOS\_AINS\_PARTIAL** At least one connection in the circuit is in the **OOS\_AINS** state and at least one other connection in the circuit is in **IS** or **OOS\_AINS** state.

[Table 1-24](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-24 Circuit in Partial State**

| Possible Problem                                                                                                                                                    | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model. | <p>Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Refer to the <a href="#">“View the State of Circuit Nodes”</a> section on page 1-65.</p> <p>Logon to the circuit node that did not change to the desired state and determine the version of software. If the software on the node is a version earlier than 3.4, upgrade the software. Refer to the <i>Cisco ONS 15454 Software Upgrade Guide</i> for software upgrade procedures.</p> <p><b>Note</b> If the node software cannot be upgraded to version 3.4, the partial state condition can be avoided by only using the circuit state(s) supported in the earlier software version.</p> |
| During an automatic transition, some path-level defects and/or alarms were detected on the circuit.                                                                 | <p>Determine which node in the circuit is not changing to the desired state. Refer to the <a href="#">“View the State of Circuit Nodes”</a> section on page 1-65.</p> <p>Logon to the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the <i>Cisco ONS 15454 Procedures Guide</i> for procedures to clear alarms and change circuit configuration settings.</p>                                                                                                                                                                                                                                                                        |
| One end of the circuit is not properly terminated.                                                                                                                  | <p>Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Procedure: View the State of Circuit Nodes

- 
- Step 1** Click the **Circuits** tab.
- Step 2** From the Circuits tab list, select the circuit with the \*\_**PARTIAL** state condition.
- Step 3** Click the **Edit** button. The Edit Circuit window appears.
- Step 4** In the Edit Circuit window, click the **State** tab.
- The State tab window will list the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.
- 

## 1.8.2 AIS-V on DS3XM-6 Unused VT Circuits

**Symptom** An incomplete circuit path causes an alarm indications signal (AIS).

[Table 1-25](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-25 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.<br>Perform the <a href="#">“Clear AIS-V on DS3XM-6 Unused VT Circuits”</a> section on page 1-66. |

## Procedure: 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.
- 

## 1.8.3 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 1-26](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-26 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 <i>Cisco ONS 15454 Reference Guide</i> for more information. |

## 1.8.4 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 1-27](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-27 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.<br><br><b>Note</b> You can find instructions for creating circuits in the <i>Cisco ONS 15454 Procedures Guide</i> . |

## 1.8.5 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 1-28](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-28 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.<br><br>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 <i>Cisco ONS 15454 Procedures Guide</i> . |

## 1.8.6 OC-3 and DCC Limitations

**Symptom** Limitations to OC-3 and DCC usage.

[Table 1-29](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-29 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 <i>Cisco ONS 15454 Procedures Guide</i> . |

## 1.8.7 ONS 15454 Switches Timing Reference

**Symptom** Timing references switch when one or more problems occur.

[Table 1-30](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-30 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 $\pm 4.6$ ppm and a holdover stability of less than 255 slips in the first 24 hours or $3.7 \times 10^{-7}$ /day, including temperature. |
| The optical or BITS input is not functioning.                                                                           | 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.                                 |
| 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.                                                                |                                                                                                                                                                                                                                                                                      |

## 1.8.8 Holdover Synchronization Alarm

**Symptom** The clock is running at a different frequency than normal and the HLDOVERSYNC alarm appears.

[Table 1-31](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-31 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 <a href="#">“HLDOVERSYNC” section on page 2-68</a> for a detailed description of this alarm.<br><br><b>Note</b> The ONS 15454 supports holdover timing per Telcordia standard GR-4436 when provisioned for external (BITS) timing. |

## 1.8.9 Free-Running Synchronization Mode

**Symptom** The clock is running at a different frequency than normal and the FRNGSYNC alarm appears.

[Table 1-32](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-32 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 <a href="#">“FRNGSYNC” section on page 2-66</a> for a detailed description of this alarm. |

## 1.8.10 Daisy-Chained BITS Not Functioning

**Symptom** You are unable to daisy-chain the BITS.

[Table 1-33](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-33 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. |

## 1.8.11 Blinking STAT LED after Installing a Card

**Symptom** After installing a card, the STAT LED blinks continuously for more than 60 seconds.

[Table 1-34](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-34** *Blinking STAT LED on installed card*

| Possible Problem                                                                   | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics. | <p>The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot.</p> <p>If the card has truly failed, an EQPT-BOOT alarm is raised against the slot number with an “Equipment Fails To Boot” description. Check the alarm tab for this alarm to appear for the slot where the card was installed.</p> <p>To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card.</p> |
|                                                                                    | <p></p> <p><b>Caution</b> Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the <i>Cisco ONS 15454 Procedure Guide</i> for information.</p>                                                                                                                                                                                                                        |

## 1.9 Fiber and Cabling

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

### 1.9.1 Bit Errors Appear for a Traffic Card

**Symptom** A traffic card has multiple Bit errors.

[Table 1-35](#) describes the potential cause(s) of the symptom and the solution(s).



**Table 1-35 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 <a href="#">“Network Troubleshooting Tests”</a> section on page 1-2. Troubleshoot low optical levels using the <a href="#">“Faulty Fiber-Optic Connections”</a> section on page 1-71. |

## 1.9.2 Faulty Fiber-Optic Connections

**Symptom** A line card has multiple SONET alarms and/or signal errors.

[Table 1-36](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-36 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 <a href="#">“Verify Fiber-Optic Connections”</a> section on page 1-71.                   |
| Faulty gigabit interface connectors. | Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the <a href="#">“Replace Faulty Gigabit Interface Converters”</a> section on page 1-73. |
| Faulty CAT-5 cables.                 | Faulty CAT-5 cables can be the source of SONET alarms and signal errors. See the <a href="#">“Crimp Replacement LAN Cables”</a> section on page 1-75.                                |



### Warning

**Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector. Class IIIb laser. Danger, laser radiation when open. The OC-192 laser is off when the safety key is off (labeled 0). The laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. Avoid direct exposure to the beam. Invisible radiation is emitted from the aperture at the end of the fiber optic cable when connected, but not terminated.**

## Procedure: Verify Fiber-Optic Connections

- 
- Step 1** Ensure that a single-mode fiber connects to the ONS 15454 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:
- Remove the receive (Rx) end of the suspect fiber.
  - Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettek LP-5000.
  - Determine the power level of fiber with the fiber-optic power meter.
  - 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).
  - Verify that the power level falls within the range specified for the card; see the [“Optical Card Transmit and Receive Levels”](#) section on page 1-77.

- Step 4** If the power level falls below the specified range:
- 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.
  - 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.
  - 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.
  - Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

**Caution**


---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

- 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.
- 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.
  - 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.
  - Retest the fiber power level.
  - If the replacement fiber still shows no power, replace the optical card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**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**

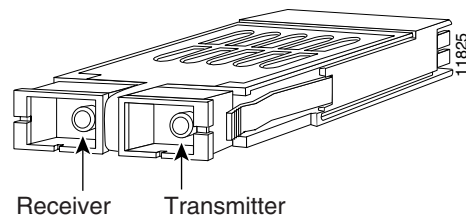
Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

## Procedure: Replace Faulty Gigabit Interface Converters

Gigabit interface converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet port to link the port with the fiber-optic network. Cisco provides two GBIC models: one for short reach applications, 15454-GBIC-SX, and one for long reach applications, 15454-GBIC-LX. The short reach, or “SX” model, connects to multimode fiber and has a maximum cabling distance of 1804 feet. The long reach, or “LX” model, requires single-mode fiber and has a maximum cabling distance of 32,810 feet.

GBICs can be installed or removed while the card and shelf assembly are powered and running. GBIC transmit failure is characterized by a steadily blinking Fail LED on the Gigabit Ethernet (E1000-2/E1000-2-G) card. [Figure 1-26](#) shows a GBIC.

**Figure 1-26** A gigabit interface converter (GBIC)

**Warning**

**Class 1 laser product**

**Warning**

---

**Invisible laser radiation may be emitted from the aperture ports of single-mode fiber optic modules when a cable is not connected. Avoid exposure and do not stare into open apertures.**

---

- Step 1** Disconnect the network interface fiber-optic cable from the GBIC SC connector and replace the protective plug.
- Step 2** Release the GBIC from the card-interface by simultaneously squeezing the two plastic tabs, one on each side of the GBIC.
- Step 3** Slide the GBIC out of the Gigabit Ethernet front-panel slot.



---

**Note** A flap closes over the GBIC slot to protect the connector on the Gigabit Ethernet (E1000-2/E1000-2-G) card.

---

- Step 4** Remove the new GBIC from its protective packaging.
- Step 5** Check the part number to verify that the GBIC is the correct type for your network.



---

**Caution** Check the label on the GBIC carefully. The two GBIC models look similar.

---

- Step 6** Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the front panel of the Gigabit Ethernet (E1000-2/E1000-2-G) card.

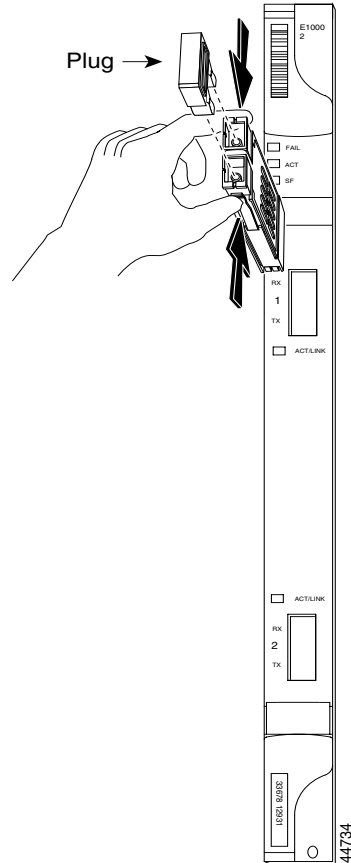


---

**Note** GBICs are keyed to prevent incorrect installation.

---

**Figure 1-27** Installing a GBIC on the E1000-2/E1000-2-G card

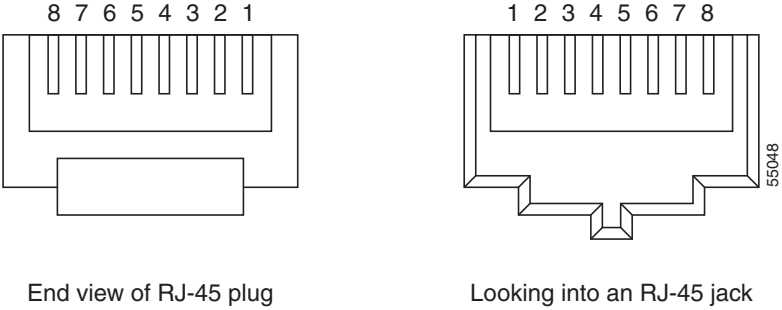


- Step 7** Slide the GBIC through the front flap until you hear a click. The click indicates that the GBIC is locked into the slot.
- Step 8** When you are ready to attach the network interface fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

## Procedure: Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use Category 5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. [Figure 1-28](#) shows the layout of an RJ-45 connector. [Figure 1-29](#) shows the layout of a LAN cable and [Figure 1-30](#) shows the layout of a cross-over cable.

Figure 1-28 RJ-45 pin numbers



End view of RJ-45 plug

Looking into an RJ-45 jack

Figure 1-29 LAN cable layout

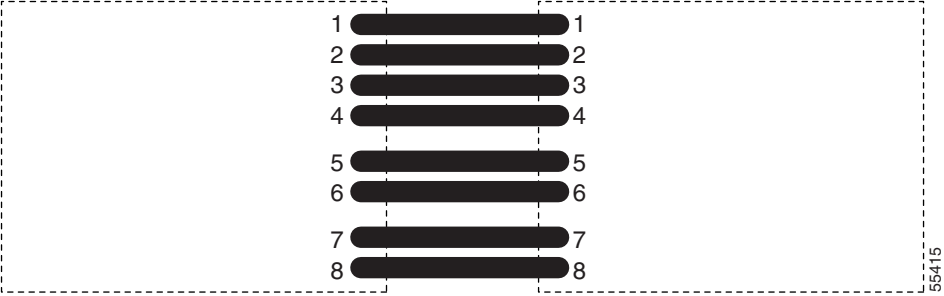


Table 1-37 LAN cable pinout

| Pin | Color        | Pair | Name            | Pin |
|-----|--------------|------|-----------------|-----|
| 1   | white/orange | 2    | Transmit Data + | 1   |
| 2   | orange       | 2    | Transmit Data - | 2   |
| 3   | white/green  | 3    | Receive Data +  | 3   |
| 4   | blue         | 1    |                 | 4   |
| 5   | white/blue   | 1    |                 | 5   |
| 6   | green        | 3    | Receive Data -  | 6   |
| 7   | white/brown  | 4    |                 | 7   |
| 8   | brown        | 4    |                 | 8   |

Figure 1-30 Cross-over cable layout

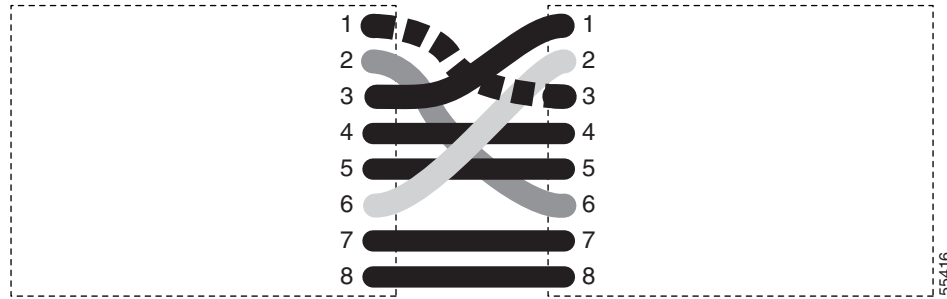


Table 1-38 Cross-over cable pinout

| Pin | Color        | Pair | Name            | Pin |
|-----|--------------|------|-----------------|-----|
| 1   | white/orange | 2    | Transmit Data + | 3   |
| 2   | orange       | 2    | Transmit Data - | 6   |
| 3   | white/green  | 3    | Receive Data +  | 1   |
| 4   | blue         | 1    |                 | 4   |
| 5   | white/blue   | 1    |                 | 5   |
| 6   | green        | 3    | Receive Data -  | 2   |
| 7   | white/brown  | 4    |                 | 7   |
| 8   | brown        | 4    |                 | 8   |

**Note**

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

## 1.9.3 Optical Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate.

Table 1-39 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  |
| OC12/STM4-4          | -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  |

**Table 1-39 Optical Card Transmit and Receive Levels (continued)**

| Optical card  | Rx            | Tx            |
|---------------|---------------|---------------|
| OC48 ELR DWDM | -8 to -28 dBm | 0 to -2 dBm   |
| OC192 LR 1550 | -9 to -17 dBm | +10 to +7 dBm |

## 1.10 Power and LED Tests

This section provides the [“Power Supply Problems”](#) section on page 1-78, the [“Power Consumption for Node and Cards”](#) section on page 1-79, and the [“Lamp Test for Card LEDs”](#) section on page 1-80.

### 1.10.1 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 1-40](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-40 Power Supply Problems**

| Possible Problem                   | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loss of power or low voltage.      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Improperly connected power supply. | <p>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.</p> <p>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 <b>Provisioning &gt; General</b> tabs and change the <i>Date</i> and <i>Time</i> fields.</p> <p>See the <a href="#">“Isolate the Cause of Power Supply Problems”</a> section on page 1-79.</p> |

**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.**



## Procedure: 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.
- 

### 1.10.2 Power Consumption for Node and Cards

**Symptom** You are unable to power up a node or the cards in a node.

[Table 1-41](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-41 Power Consumption for Node and Cards**

| Possible Problem       | Solution                                                                   |
|------------------------|----------------------------------------------------------------------------|
| Improper power supply. | Refer to power information in the <i>Cisco ONS 15454 Procedure Guide</i> . |

## 1.10.3 Lamp Test for Card LEDs

**Symptom** Card LED will not light or you are unsure if LEDs are working properly.

[Table 1-42](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 1-42 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.<br><br>See the <a href="#">“Verify Card LED Operation”</a> section on page 1-80. |

### Procedure: Verify Card LED Operation

- 
- Step 1** Click the **Maintenance > Diagnostic** tabs.
  - Step 2** Click **Lamp Test**.
  - Step 3** Watch to make sure all the LEDs on the cards illuminate for several seconds.
  - Step 4** Click **OK** on the Lamp Test Run dialog box.

If an LED does not light up, the LED is faulty. Call the Cisco TAC at 1-877-323-7368 and fill out an RMA to return the card.

---



## Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each Cisco ONS 15454 alarm and conditions commonly encountered while troubleshooting major alarms. [Table 2-5 on page 2-4](#) gives an alphabetical list of alarms that appear on the ONS 15454. [Table 2-6 on page 2-6](#) gives a list of alarms organized by alarm type. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and ONS 15327 TLI Command Guide*.

The troubleshooting procedure for an alarm applies to both the CTC and TLI 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 on unprovisioned card ports 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. Alarm severities can be altered from default settings for individual alarms or groups of alarms on a card, node, or network basis. These alterations can be made using NTP-71 Create, Download, and Assign Alarm Severity Profiles in the *Cisco ONS 15454 Procedure Guide*.

### 2.1 Alarm Index by Default Severity

The alarm index by severity groups alarms and conditions by the severity displayed in the CTC Alarms tab in the severity (SEV) column. You can change the severity of any alarm by creating an alarm profile. See the *Cisco ONS 15454 Procedure Guide* for alarm profile procedures.



**Note**

The CTC default alarm profile contains alarms that apply to multiple product platforms. The alarms that apply to this product are listed in the following tables and sections.

#### 2.1.1 Critical Alarms (CR)

**Table 2-1 Critical Alarm Index**

|                                       |                                       |                                         |
|---------------------------------------|---------------------------------------|-----------------------------------------|
| <a href="#">AUTOLSROFF, page 2-24</a> | <a href="#">HITEMP, page 2-67</a>     | <a href="#">MEA (Bplane), page 2-89</a> |
| <a href="#">BKUPMEMP, page 2-27</a>   | <a href="#">IMPROPRMVL, page 2-69</a> | <a href="#">MEA (EQPT), page 2-90</a>   |
| <a href="#">COMIOXC, page 2-34</a>    | <a href="#">LOF (DS3), page 2-74</a>  | <a href="#">MEA (FAN), page 2-92</a>    |

**Table 2-1 Critical Alarm Index (continued)**

|                           |                         |                      |
|---------------------------|-------------------------|----------------------|
| CONCAT, page 2-35         | LOF (EC1-12), page 2-75 | MFGMEM, page 2-93x   |
| CTNEQPT-PBPROT, page 2-39 | LOF (OC-N), page 2-75   | PLM-P, page 2-96     |
| CTNEQPT-PBWORK, page 2-40 | LOP-P, page 2-76        | SWMTXMOD, page 2-116 |
| EQPT, page 2-46           | LOS (EC1-12), page 2-81 | TIM-P, page 2-121    |
| EQPT-MISS, page 2-47      | LOS (OC-N), page 2-82   | UNEQ-P, page 2-124   |
| FAN, page 2-55            | MEA (AIP), page 2-89    |                      |

## 2.1.2 Major Alarms (MJ)

**Table 2-2 Major Alarm Index**

|                               |                         |                            |
|-------------------------------|-------------------------|----------------------------|
| APSCM, page 2-20              | ELWBATVG-B, page 2-44   | PEER-NORESPONSE, page 2-96 |
| APSCNMIS, page 2-21           | EOC, page 2-44          | PRC-DUPID, page 2-98       |
| BLSROSYNC, page 2-28          | E-W-MISMATCH, page 2-47 | PWR-A, page 2-100          |
| CARLOSS (EQPT), page 2-28     | FRNGSYNC, page 2-66     | PWR-B, page 2-100          |
| CARLOSS (E-Series), page 2-29 | HLDOVRSYNC, page 2-68   | RCVR-MISS, page 2-101      |
| CARLOSS (G1000-4), page 2-31  | INVMACADR, page 2-71    | RING-MISMATCH, page 2-104  |
| CONTBUS-A-18, page 2-35       | LOF (BITS), page 2-73   | SYSBOOT, page 2-121        |
| CONTBUS-B-18, page 2-36       | LOF (DS1), page 2-74    | TPTFAIL, page 2-122        |
| CONTBUS-IO-A, page 2-37       | LOP-V, page 2-77        | TRMT, page 2-122           |
| CONTBUS-IO-B, page 2-38       | LOS (BITS), page 2-79   | TRMT-MISS, page 2-123      |
| EHIBATVG-A, page 2-43         | LOS (DS-1), page 2-79   | UNEQ-P, page 2-124         |
| EHIBATVG-B, page 2-43         | LOF (DS3), page 2-74    | UNEQ-V, page 2-125         |
| ELWBATVG-A, page 2-43         | MEM-GONE, page 2-93     |                            |

## 2.1.3 Minor Alarms (MN)

**Table 2-3 Minor Alarm Index**

|                                 |                                 |                       |
|---------------------------------|---------------------------------|-----------------------|
| APSB, page 2-18                 | AUTOSW-UNEQ (VT-MON), page 2-27 | PROTNA, page 2-99     |
| APSCDFLTK, page 2-18            | DATAFLT, page 2-42              | SFTWDOWN, page 2-110  |
| APSC-IMP, page 2-19             | EXCCOL, page 2-49               | SNTP-HOST, page 2-110 |
| APSCDFLTK, page 2-18            | EXT, page 2-50                  | SSM-FAIL, page 2-113  |
| APSCINCON, page 2-20            | FEPRLF, page 2-64               | SYNCPRI, page 2-119   |
| APSMM, page 2-22                | FSTSYNC, page 2-67              | SYNCSEC, page 2-119   |
| AUTORESET, page 2-25x           | MEM-LOW, page 2-93              | SYNCTHIRD, page 2-120 |
| AUTOSW-LOP (VT-MON), page 2-26x | PLM-V, page 2-98                |                       |

## 2.1.4 Conditions (NA or NR)

**Table 2-4** Conditions Index

|                                                 |                                                              |                                            |
|-------------------------------------------------|--------------------------------------------------------------|--------------------------------------------|
| <a href="#">AIS, page 2-16</a>                  | <a href="#">FE-LOF, page 2-62</a>                            | <a href="#">MANSWTOTHIRD, page 2-89</a>    |
| <a href="#">AIS-L, page 2-16</a>                | <a href="#">FE-LOS, page 2-63</a>                            | <a href="#">MANUAL-REQ-RING, page 2-89</a> |
| <a href="#">AIS-P, page 2-16</a>                | <a href="#">FE-MANWKSWPR-RING, page 2-63</a>                 | <a href="#">MANUAL-REQ-SPAN, page 2-89</a> |
| <a href="#">AIS-V, page 2-17</a>                | <a href="#">FE-MANWKSWPR-SPAN, page 2-64</a>                 | <a href="#">PDI-P, page 2-94</a>           |
| <a href="#">AS-CMD, page 2-22</a>               | <a href="#">FORCED-REQ, page 2-65</a>                        | <a href="#">RAI, page 2-101</a>            |
| <a href="#">AS-MT, page 2-23</a>                | <a href="#">FORCED-REQ-RING, page 2-65</a>                   | <a href="#">RFI-L, page 2-102</a>          |
| <a href="#">AUTOSW-AIS, page 2-25</a>           | <a href="#">FORCED-REQ-SPAN, page 2-65</a>                   | <a href="#">RFI-P, page 2-102</a>          |
| <a href="#">AUTOSW-LOP (STSMON), page 2-25</a>  | <a href="#">FRCDSWTOINT, page 2-65</a>                       | <a href="#">RFI-V, page 2-103</a>          |
| <a href="#">AUTOSW-PDI, page 2-26</a>           | <a href="#">FRCDSWTOPRI, page 2-66</a>                       | <a href="#">RING-SW-EAST, page 2-104</a>   |
| <a href="#">AUTOSW-SDBER, page 2-26</a>         | <a href="#">FRCDSWTOSEC, page 2-66</a>                       | <a href="#">RING-SW-WEST, page 2-104</a>   |
| <a href="#">AUTOSW-SFBER, page 2-26</a>         | <a href="#">FRCDSWTOHIRD, page 2-66</a>                      | <a href="#">SD-L, page 2-105</a>           |
| <a href="#">AUTOSW-UNEQ (STSMON), page 2-27</a> | <a href="#">FULLPASSTHR-BI, page 2-67</a>                    | <a href="#">SD-P, page 2-106</a>           |
| <a href="#">CLDRESTART, page 2-33</a>           | <a href="#">INC-ISD, page 2-70</a>                           | <a href="#">SF-L, page 2-107</a>           |
| <a href="#">DS3-MISM, page 2-42</a>             | <a href="#">INHSWPR, page 2-70</a>                           | <a href="#">SF-P, page 2-108</a>           |
| <a href="#">EXERCISE-RING-REQ, page 2-49</a>    | <a href="#">INHSWKG, page 2-71</a>                           | <a href="#">SPAN-SW-EAST, page 2-110</a>   |
| <a href="#">EXERCISE-SPAN-REQ, page 2-50</a>    | <a href="#">KB-PASSTHR, page 2-72</a>                        | <a href="#">SPAN-SW-WEST, page 2-111</a>   |
| <a href="#">EXTRA-TRAF-PREEMPT, page 2-50</a>   | <a href="#">LKOUTPR-S, page 2-72</a>                         | <a href="#">SQUELCH, page 2-111</a>        |
| <a href="#">FAILTOSW, page 2-51</a>             | <a href="#">LOCKOUT-REQ, page 2-72</a>                       | <a href="#">SSM-DUS, page 2-112</a>        |
| <a href="#">FAILTOSW-PATH, page 2-51</a>        | <a href="#">LOCKOUT-REQ-RING, page 2-72</a>                  | <a href="#">SSM-OFF, page 2-113</a>        |
| <a href="#">FAILTOSWR, page 2-53</a>            | <a href="#">LOCKOUT-REQ-SPAN, page 2-72</a>                  | <a href="#">SSM-PRS, page 2-113</a>        |
| <a href="#">FAILTOSWS, page 2-55</a>            | <a href="#">LPBKDS1FEAC, page 2-84</a>                       | <a href="#">SSM-RES, page 2-114</a>        |
| <a href="#">FE-AIS, page 2-56</a>               | <a href="#">LPBKDS3FEAC-CMD, page 2-85</a>                   | <a href="#">SSM-SMC, page 2-114</a>        |
| <a href="#">FE-DS1-MULTLOS, page 2-56</a>       | <a href="#">LPBKDS3FEAC, page 2-85</a>                       | <a href="#">SSM-ST2, page 2-114</a>        |
| <a href="#">FE-DS1-NSA, page 2-57</a>           | <a href="#">LPBKDS3FEAC-CMD, page 2-85</a>                   | <a href="#">SSM-ST3, page 2-114</a>        |
| <a href="#">FE-DS1-SA, page 2-57</a>            | <a href="#">LPBKFACILITY (DS-N or EC1-12), page 2-85</a>     | <a href="#">SSM-ST3E, page 2-115</a>       |
| <a href="#">FE-DS1-SNGLLOS, page 2-58</a>       | <a href="#">LPBKFACILITY (OC-N), page 2-86</a>               | <a href="#">SSM-ST4, page 2-115</a>        |
| <a href="#">FE-DS3-NSA, page 2-58</a>           | <a href="#">LPBKTERMINAL (DS-N, EC1-12, OC-N), page 2-87</a> | <a href="#">SSM-TNC, page 2-116</a>        |
| <a href="#">FE-DS3-SA, page 2-59</a>            | <a href="#">LPBKTERMINAL(G1000-4), page 2-87</a>             | <a href="#">SSM-STU, page 2-115</a>        |
| <a href="#">FE-EQPT-NSA, page 2-59</a>          | <a href="#">MAN-REQ, page 2-87</a>                           | <a href="#">SWTOPRI, page 2-118</a>        |
| <a href="#">FE-EXERCISING-RING, page 2-60</a>   | <a href="#">MANRESET, page 2-88</a>                          | <a href="#">SWTOSEC, page 2-118</a>        |
| <a href="#">FE-EXERCISING-SPAN, page 2-60</a>   | <a href="#">MANUAL-REQ-RING, page 2-89</a>                   | <a href="#">SWTOHIRD, page 2-118</a>       |
| <a href="#">FE-FRCDWKSWPR-RING, page 2-60</a>   | <a href="#">MANUAL-REQ-SPAN, page 2-89</a>                   | <a href="#">SYNC-FREQ, page 2-118</a>      |
| <a href="#">FE-FRCDWKSWPR-SPAN, page 2-61</a>   | <a href="#">MANSWTOINT, page 2-88</a>                        | <a href="#">WKSWPR, page 2-127</a>         |

Table 2-4 Conditions Index (continued)

|                                |                       |                 |
|--------------------------------|-----------------------|-----------------|
| FE-IDLE, page 2-61             | MANSWTOPRI, page 2-88 | WTR, page 2-127 |
| FE-LOCKOUTOFPR-SPAN, page 2-62 | MANSWTOSEC, page 2-88 |                 |

## 2.2 Alarm Index By Alphabetical Entry

The following table lists alarms by the name displayed on the CTC Alarms tab in the conditions column.

Table 2-5 Alarm Index

|                                 |                                |                            |
|---------------------------------|--------------------------------|----------------------------|
| AIS, page 2-16                  | FE-EQPT-NSA, page 2-59         | MANUAL-REQ-SPAN, page 2-89 |
| AIS-L, page 2-16                | FE-EXERCISING-RING, page 2-60  | MEA (AIP), page 2-89       |
| AIS-P, page 2-16                | FE-EXERCISING-SPAN, page 2-60  | MEA (Bplane), page 2-89    |
| AIS-V, page 2-17                | FE-FRCDWKSWPR-RING, page 2-60  | MEA (EQPT), page 2-90      |
| APSB, page 2-18                 | FE-FRCDWKSWPR-SPAN, page 2-61  | MEM-GONE, page 2-93        |
| APSCDFLTK, page 2-18            | FE-IDLE, page 2-61             | MEM-LOW, page 2-93         |
| APSC-IMP, page 2-19             | FE-LOCKOUTOFPR-SPAN, page 2-62 | MFGMEM, page 2-93          |
| APSCINCON, page 2-20            | FE-LOF, page 2-62              | PDI-P, page 2-94           |
| APSCM, page 2-20                | FE-LOS, page 2-63              | PEER-NORESPONSE, page 2-96 |
| APSCNMIS, page 2-21             | FE-MANWKSWPR-RING, page 2-63   | PLM-P, page 2-96           |
| APSM, page 2-22                 | FE-MANWKSWPR-SPAN, page 2-64   | PLM-V, page 2-98           |
| AS-CMD, page 2-22               | FEPRLF, page 2-64              | PRC-DUPID, page 2-98       |
| AS-MT, page 2-23                | FORCED-REQ, page 2-65          | PWR-A, page 2-100          |
| AUTOLSROFF, page 2-24           | FORCED-REQ-RING, page 2-65     | PWR-B, page 2-100          |
| AUTORESET, page 2-25            | FORCED-REQ-SPAN, page 2-65     | RAI, page 2-101            |
| AUTOSW-AIS, page 2-25           | FRCDSWTOINT, page 2-65         | RCVR-MISS, page 2-101      |
| AUTOSW-LOP (STSMON), page 2-25  | FRCDSWTOPRI, page 2-66         | RFI-L, page 2-102          |
| AUTOSW-LOP (VT-MON), page 2-26  | FRCDSWTOSEC, page 2-66         | RFI-V, page 2-103          |
| AUTOSW-PDI, page 2-26           | FRCDSWTOTHIRD, page 2-66       | RING-MISMATCH, page 2-104  |
| AUTOSW-SDBER, page 2-26         | FRNGSYNC, page 2-66            | RING-SW-EAST, page 2-104   |
| AUTOSW-SFBER, page 2-26         | FSTSYNC, page 2-67             | RING-SW-WEST, page 2-104   |
| AUTOSW-UNEQ (STSMON), page 2-27 | FULLPASSTHR-BI, page 2-67      | SD-L, page 2-105           |
| AUTOSW-UNEQ (VT-MON), page 2-27 | HITEMP, page 2-67              | SD-P, page 2-106           |
| BKUPMEM, page 2-27              | HLDOVRSYNC, page 2-68          | SF-L, page 2-107           |
| BLSROSYNC, page 2-28            | IMPROPRMVL, page 2-69          | SF-P, page 2-108           |
| CARLOSS (E-Series), page 2-29   | INC-ISD, page 2-70             | SFTWDOWN, page 2-110       |
| CLDRESTART, page 2-33           | INHWSWPR, page 2-70            | SNTP-HOST, page 2-110      |

Table 2-5 Alarm Index (continued)

|                              |                                                 |                          |
|------------------------------|-------------------------------------------------|--------------------------|
| COMIOXC, page 2-34           | INHSSWWKG, page 2-71                            | SPAN-SW-EAST, page 2-110 |
| CONCAT, page 2-35            | INVMACADR, page 2-71                            | SPAN-SW-WEST, page 2-111 |
| CONTBUS-A-18, page 2-35      | KB-PASSTHR, page 2-72                           | SQUELCH, page 2-111      |
| CONTBUS-B-18, page 2-36      | LKOUTPR-S, page 2-72                            | SSM-DUS, page 2-112      |
| CONTBUS-IO-A, page 2-37      | LOCKOUT-REQ, page 2-72                          | SSM-FAIL, page 2-113     |
| CONTBUS-IO-B, page 2-38      | LOCKOUT-REQ-RING, page 2-72                     | SSM-OFF, page 2-113      |
| CTNEQPT-PBPROT, page 2-39    | LOF (BITS), page 2-73                           | SSM-PRS, page 2-113      |
| CTNEQPT-PBWORK, page 2-40    | LOF (DS1), page 2-74                            | SSM-RES, page 2-114      |
| DATAFLT, page 2-42           | LOF (DS3), page 2-74                            | SSM-SMC, page 2-114      |
| DS3-MISM, page 2-42          | LOF (EC1-12), page 2-75                         | SSM-STU, page 2-115      |
| EHIBATVG-A, page 2-43        | LOF (OC-N), page 2-75                           | SSM-ST2, page 2-114      |
| EHIBATVG-B, page 2-43        | LOP-P, page 2-76                                | SSM-ST3, page 2-114      |
| ELWBATVG-A, page 2-43        | LOP-V, page 2-77                                | SSM-ST3E, page 2-115     |
| ELWBATVG-B, page 2-44        | LOS (BITS), page 2-79                           | SSM-ST4, page 2-115      |
| EOC, page 2-44               | LOS (DS-1), page 2-79                           | SSM-TNC, page 2-116      |
| EQPT, page 2-46              | LOS (EC1-12), page 2-81                         | SWMTXMOD, page 2-116     |
| EQPT-MISS, page 2-47         | LOS (OC-N), page 2-82                           | SWTOPRI, page 2-118      |
| E-W-MISMATCH, page 2-47      | LOS (OC-N), page 2-82                           | SWTOSEC, page 2-118      |
| EXCCOL, page 2-49            | LOS (OC-N), page 2-82                           | SWTOTHIRD, page 2-118    |
| EXERCISE-RING-REQ, page 2-49 | LPBKDS1FEAC, page 2-84                          | SYNC-FREQ, page 2-118    |
| EXERCISE-SPAN-REQ, page 2-50 | LPBKDS1FEAC-CMD, page 2-84                      | SYNCPRI, page 2-119      |
| EXT, page 2-50               | LPBKDS3FEAC, page 2-85                          | SYNCSEC, page 2-119      |
| FAILTOSW, page 2-51          | LPBKDS3FEAC-CMD, page 2-85                      | SYNCTHIRD, page 2-120    |
| FAILTOSW-PATH, page 2-51     | LPBKFACILITY (DS-N or EC1-12),<br>page 2-85     | SYSBOOT, page 2-121      |
| FAILTOSWR, page 2-53         | LPBKFACILITY (OC-N), page 2-86                  | TIM-P, page 2-121        |
| FAILTOSWS, page 2-55         | LPBKTERMINAL (DS-N, EC1-12,<br>OC-N), page 2-87 | TPTFAIL, page 2-122      |
| FAN, page 2-55               | MAN-REQ, page 2-87                              | TRMT, page 2-122         |
| FE-AIS, page 2-56            | MANRESET, page 2-88                             | TRMT-MISS, page 2-123    |
| FE-DS1-MULTLOS, page 2-56    | MANSWTOINT, page 2-88                           | UNEQ-P, page 2-124       |
| FE-DS1-NSA, page 2-57        | MANSWTOPRI, page 2-88                           | UNEQ-P, page 2-124       |
| FE-DS1-SA, page 2-57         | MANSWTOSEC, page 2-88                           | UNEQ-V, page 2-125       |
| FE-DS1-SNGLLOS, page 2-58    | MANSWTOHIRD, page 2-89                          | WKSWPR, page 2-127       |
| FE-DS3-NSA, page 2-58        | MANUAL-REQ-RING, page 2-89                      | WTR, page 2-127          |
| FE-DS3-SA, page 2-59         |                                                 |                          |

## 2.3 Alarm Index by Alarm Type

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

**Table 2-6 Alarm Index by Alarm Type**

|                                                   |
|---------------------------------------------------|
| AIP::EQPT, page 2-46                              |
| AIP::INVMACADR, page 2-71                         |
| AIP::MEA (AIP), page 2-89                         |
| AIP::MFGMEM, page 2-93                            |
| AEP::MFGMEM, page 2-93                            |
| BITS::AIS, page 2-16                              |
| BITS::LOF (BITS), page 2-73                       |
| BITS::LOS (BITS), page 2-79                       |
| BITS::SSM-DUS, page 2-112                         |
| BITS::SSM-FAIL, page 2-113                        |
| BITS::SSM-OFF, page 2-113                         |
| BITS::SSM-PRS, page 2-113                         |
| BITS::SSM-RES, page 2-114                         |
| BITS::SSM-SMC, page 2-114                         |
| BITS::SSM-ST2, page 2-114                         |
| BITS::SSM-ST3, page 2-114                         |
| BITS::SSM-ST3E, page 2-115                        |
| BITS::SSM-ST4, page 2-115                         |
| BITS::SSM-STU, page 2-115                         |
| BITS::SSM-TNC, page 2-116                         |
| BITS::SYNC-FREQ, page 2-118                       |
| BPLANE::AS-CMD, page 2-22                         |
| BPLANE::MEA (Bplane), page 2-89                   |
| BPLANE::MFGMEM, page 2-93                         |
| DS1::AIS, page 2-16                               |
| DS1::AS-CMD, page 2-22                            |
| DS1::AS-MT, page 2-23                             |
| DS1::LOF (DS1), page 2-74                         |
| DS1::LOS (DS-1), page 2-79                        |
| DS1::LPBKDS1FEAC, page 2-84                       |
| DS1::LPBKDS1FEAC-CMD, page 2-84                   |
| DS1::LPBKFACILITY (DS-N or EC1-12), page 2-85     |
| DS1::LPBKTERMINAL (DS-N, EC1-12, OC-N), page 2-87 |



**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                                                   |
|-------------------------------------------------------------------|
| <a href="#">DS1::RAI, page 2-101</a>                              |
| <a href="#">DS1::RCVR-MISS, page 2-101</a>                        |
| <a href="#">DS1::TRMT, page 2-122</a>                             |
| <a href="#">DS1::TRMT-MISS, page 2-123</a>                        |
| <a href="#">DS3::AIS, page 2-16</a>                               |
| <a href="#">DS3::AS-CMD, page 2-22</a>                            |
| <a href="#">DS3::AS-MT, page 2-23</a>                             |
| <a href="#">DS3::DS3-MISM, page 2-42</a>                          |
| <a href="#">DS3::FE-AIS, page 2-56</a>                            |
| <a href="#">DS3::FE-DS1-MULTLOS, page 2-56</a>                    |
| <a href="#">DS3::FE-DS1-NSA, page 2-57</a>                        |
| <a href="#">DS3::FE-DS1-SA, page 2-57</a>                         |
| <a href="#">DS3::FE-DS1-SNGLLOS, page 2-58</a>                    |
| <a href="#">DS3::FE-DS3-NSA, page 2-58</a>                        |
| <a href="#">DS3::FE-DS3-SA, page 2-59</a>                         |
| <a href="#">DS3::FE-EQPT-NSA, page 2-59</a>                       |
| <a href="#">DS3::FE-IDLE, page 2-61</a>                           |
| <a href="#">DS3::FE-LOF, page 2-62</a>                            |
| <a href="#">DS3::FE-LOS, page 2-63</a>                            |
| <a href="#">DS3::INC-ISD, page 2-70</a>                           |
| <a href="#">DS3::LOF (DS3), page 2-74</a>                         |
| <a href="#">DS3::LOS (DS-3), page 2-80</a>                        |
| <a href="#">DS3::LPBKDS1FEAC, page 2-84</a>                       |
| <a href="#">DS3::LPBKDS3FEAC, page 2-85</a>                       |
| <a href="#">DS3::LPBKDS3FEAC-CMD, page 2-85</a>                   |
| <a href="#">DS3::LPBKFACILITY (DS-N or EC1-12), page 2-85</a>     |
| <a href="#">DS3::LPBKTERMINAL (DS-N, EC1-12, OC-N), page 2-87</a> |
| <a href="#">DS3::RAI, page 2-101</a>                              |
| <a href="#">ECN::AIS-L, page 2-16</a>                             |
| <a href="#">ECN::AS-CMD, page 2-22</a>                            |
| <a href="#">ECN::AS-MT, page 2-23</a>                             |
| <a href="#">ECN::LOF (EC1-12), page 2-75</a>                      |
| <a href="#">ECN::LPBKFACILITY (DS-N or EC1-12), page 2-85</a>     |
| <a href="#">ECN::LPBKTERMINAL (DS-N, EC1-12, OC-N), page 2-87</a> |
| <a href="#">ECN::LOS (EC1-12), page 2-81</a>                      |
| <a href="#">ENV::EXT, page 2-50</a>                               |
| <a href="#">EQPT::AS-CMD, page 2-22</a>                           |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                                       |
|-------------------------------------------------------|
| <a href="#">EQPT::AUTORESET</a> , page 2-25           |
| <a href="#">EQPT::BKUPMEMP</a> , page 2-27            |
| <a href="#">EQPT::CARLOSS (EQPT)</a> , page 2-28      |
| <a href="#">EQPT::CLDRESTART</a> , page 2-33          |
| <a href="#">EQPT::COMIOXC</a> , page 2-34             |
| <a href="#">EQPT::CONTBUS-A-18</a> , page 2-35        |
| <a href="#">EQPT::CONTBUS-B-18</a> , page 2-36        |
| <a href="#">EQPT::CONTBUS-IO-A</a> , page 2-37        |
| <a href="#">EQPT::CONTBUS-IO-B</a> , page 2-38        |
| <a href="#">EQPT::CTNEQPT-PBPROT</a> , page 2-39      |
| <a href="#">EQPT::CTNEQPT-PBWORK</a> , page 2-40      |
| <a href="#">EQPT::EQPT</a> , page 2-46                |
| <a href="#">EQPT::EXCCOL</a> , page 2-49              |
| <a href="#">EQPT::FAILTOSW</a> , page 2-51            |
| <a href="#">EQPT::FORCED-REQ</a> , page 2-65          |
| <a href="#">EQPT::HITEMP</a> , page 2-67              |
| <a href="#">EQPT::IMPROPRMVL</a> , page 2-69          |
| <a href="#">EQPT::INHSWPR</a> , page 2-70             |
| <a href="#">EQPT::INHSWWKG</a> , page 2-71            |
| <a href="#">EQPT::LOCKOUT-REQ</a> , page 2-72         |
| <a href="#">EQPT::MAN-REQ</a> , page 2-87             |
| <a href="#">EQPT::MANRESET</a> , page 2-88            |
| <a href="#">EQPT::MEA (EQPT)</a> , page 2-90          |
| <a href="#">EQPT::MEM-GONE</a> , page 2-93            |
| <a href="#">EQPT::MEM-LOW</a> , page 2-93             |
| <a href="#">EQPT::PEER-NORESPONSE</a> , page 2-96     |
| <a href="#">EQPT::PROTNA</a> , page 2-99              |
| <a href="#">EQPT::SFTWDOWN</a> , page 2-110           |
| <a href="#">EQPT::SWMTXMOD</a> , page 2-116           |
| <a href="#">EQPT::WKSWPR</a> , page 2-127             |
| <a href="#">EQPT::WTR</a> , page 2-127                |
| <a href="#">ETHER::CARLOSS (E-Series)</a> , page 2-29 |
| <a href="#">EXTSYNCH::FRCDSWTOPRI</a> , page 2-66     |
| <a href="#">EXTSYNCH::FRCDSWTOSEC</a> , page 2-66     |
| <a href="#">EXTSYNCH::FRCDSWTOHOLD</a> , page 2-66    |
| <a href="#">EXTSYNCH::MANSWTOPRI</a> , page 2-88      |
| <a href="#">EXTSYNCH::MANSWTOSEC</a> , page 2-88      |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                                                             |
|-----------------------------------------------------------------------------|
| <a href="#">EXTSYNCH::MANSWTOTHIRD</a> , page 2-89                          |
| <a href="#">EXTSYNCH::SWTOPRI</a> , page 2-118                              |
| <a href="#">EXTSYNCH::SWTOSEC</a> , page 2-118                              |
| <a href="#">EXTSYNCH::SWTOTHIRD</a> , page 2-118                            |
| <a href="#">EXTSYNCH::SYNCPRI</a> , page 2-119                              |
| <a href="#">EXTSYNCH::SYNCSEC</a> , page 2-119                              |
| <a href="#">EXTSYNCH::SYNCTHIRD</a> , page 2-120                            |
| <a href="#">FAN::EQPT-MISS</a> , page 2-47                                  |
| <a href="#">FAN::FAN</a> , page 2-55                                        |
| <a href="#">FAN::MEA (FAN)</a> , page 2-92                                  |
| <a href="#">FAN::MFGMEM</a> , page 2-93                                     |
| <a href="#">FUDC::AIS</a> , page 2-16                                       |
| <a href="#">FUDC::LOF (OC-N)</a> , page 2-75                                |
| <a href="#">HDGE [G1000]::CARLOSS (G1000-4)</a> , page 2-31                 |
| <a href="#">HDGE [G1000]::LPBKTERMINAL (DS-N, EC1-12, OC-N)</a> , page 2-87 |
| <a href="#">HDGE [G1000]::TPTFAIL</a> , page 2-122                          |
| <a href="#">NE::AS-CMD</a> , page 2-22                                      |
| <a href="#">NE::DATAFLT</a> , page 2-42                                     |
| <a href="#">NE::EHIBATVG-A</a> , page 2-43                                  |
| <a href="#">NE::EHIBATVG-B</a> , page 2-43                                  |
| <a href="#">NE::ELWBATVG-A</a> , page 2-43                                  |
| <a href="#">NE::ELWBATVG-B</a> , page 2-44                                  |
| <a href="#">NE::HITEMP</a> , page 2-67                                      |
| <a href="#">NE::PRC-DUPID</a> , page 2-98                                   |
| <a href="#">NE::PWR-A</a> , page 2-100                                      |
| <a href="#">NE::PWR-B</a> , page 2-100                                      |
| <a href="#">NE::SNTP-HOST</a> , page 2-110                                  |
| <a href="#">NE::SYSBOOT</a> , page 2-121                                    |
| <a href="#">NERING::BLSROSYNC</a> , page 2-28                               |
| <a href="#">NERING::FULLPASSTHR-BI</a> , page 2-67                          |
| <a href="#">NERING::KB-PASSTHR</a> , page 2-72                              |
| <a href="#">NERING::PRC-DUPID</a> , page 2-98                               |
| <a href="#">NERING::RING-MISMATCH</a> , page 2-104                          |
| <a href="#">NESYNCH::FRCDSWTOINT</a> , page 2-65                            |
| <a href="#">NESYNCH::FRCDSWTOPRI</a> , page 2-66                            |
| <a href="#">NESYNCH::FRCDSWTOSEC</a> , page 2-66                            |
| <a href="#">NESYNCH::FRCDSWTOTHIRD</a> , page 2-66                          |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                    |
|------------------------------------|
| NESYNCH::FRNGSYNC, page 2-66       |
| NESYNCH::FSTSYNC, page 2-67        |
| NESYNCH::HLDVRSYNC, page 2-68      |
| NESYNCH::MANSWTOINT, page 2-88     |
| NESYNCH::MANSWTOPRI, page 2-88     |
| NESYNCH::MANSWTOSEC, page 2-88     |
| NESYNCH::MANSWTOTHIRD, page 2-89   |
| NESYNCH::SSM-SMC, page 2-114       |
| NESYNCH::SSM-ST3E, page 2-115      |
| NESYNCH::SSM-ST4, page 2-115       |
| NESYNCH::SSM-STU, page 2-115       |
| NESYNCH::SSM-TNC, page 2-116       |
| NESYNCH::SWTOPRI, page 2-118       |
| NESYNCH::SWTOSEC, page 2-118       |
| NESYNCH::SWTOTHIRD, page 2-118     |
| NESYNCH::SYNCPRI, page 2-119       |
| NESYNCH::SYNCSEC, page 2-119       |
| NESYNCH::SYNCTHIRD, page 2-120     |
| OCN::AIS-L, page 2-16              |
| OCN::APSB, page 2-18               |
| OCN::APSCDFLTK, page 2-18          |
| OCN::APSC-IMP, page 2-19           |
| OCN::APSCINCON, page 2-20          |
| OCN::APSCM, page 2-20              |
| OCN::APSCNMIS, page 2-21           |
| OCN::APSCMM, page 2-22             |
| OCN::AS-CMD, page 2-22             |
| OCN::AS-MT, page 2-23              |
| OCN::AUTOLSROFF, page 2-24         |
| OCN::EOC, page 2-44                |
| OCN::E-W-MISMATCH, page 2-47       |
| OCN::EXERCISE-RING-REQ, page 2-49  |
| OCN::EXERCISE-SPAN-REQ, page 2-50  |
| OCN::EXTRA-TRAF-PREEMPT, page 2-50 |
| OCN::FAILTOSW, page 2-51           |
| OCN::FAILTOSWR, page 2-53          |
| OCN::FAILTOSWS, page 2-55          |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                                   |
|---------------------------------------------------|
| OCN::FE-EXERCISING-RING, page 2-60                |
| OCN::FE-EXERCISING-SPAN, page 2-60                |
| OCN::FE-FRCDWKSWPR-RING, page 2-60                |
| OCN::FE-FRCDWKSWPR-SPAN, page 2-61                |
| OCN::FE-LOCKOUTOFPR-SPAN, page 2-62               |
| OCN::FE-MANWKSWPR-RING, page 2-63                 |
| OCN::FE-MANWKSWPR-SPAN, page 2-64                 |
| OCN::FEPRLF, page 2-64                            |
| OCN::FORCED-REQ, page 2-65                        |
| OCN::FORCED-REQ-RING, page 2-65                   |
| OCN::FORCED-REQ-SPAN, page 2-65                   |
| OCN::LKOUTPR-S, page 2-72                         |
| OCN::LOCKOUT-REQ, page 2-72                       |
| OCN::LOCKOUT-REQ-RING, page 2-72                  |
| OCN::LOF (OC-N), page 2-75                        |
| OCN::LOS (OC-N), page 2-82                        |
| OCN::LPBKFACILITY (OC-N), page 2-86               |
| OCN::LPBKTERMINAL (DS-N, EC1-12, OC-N), page 2-87 |
| OCN::MANUAL-REQ-RING, page 2-89                   |
| OCN::MANUAL-REQ-SPAN, page 2-89                   |
| OCN::RFI-L, page 2-102                            |
| OCN::RING-SW-EAST, page 2-104                     |
| OCN::RING-SW-WEST, page 2-104                     |
| OCN::SD-L, page 2-105                             |
| OCN::SF-L, page 2-107                             |
| OCN::SPAN-SW-EAST, page 2-110                     |
| OCN::SPAN-SW-WEST, page 2-111                     |
| OCN::SQUELCH, page 2-111                          |
| OCN::SSM-DUS, page 2-112                          |
| OCN::SSM-FAIL, page 2-113                         |
| OCN::SSM-OFF, page 2-113                          |
| OCN::SSM-PRS, page 2-113                          |
| OCN::SSM-RES, page 2-114                          |
| OCN::SSM-SMC, page 2-114                          |
| OCN::SSM-ST2, page 2-114                          |
| OCN::SSM-ST3, page 2-114                          |
| OCN::SSM-ST3E, page 2-115                         |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                         |
|-----------------------------------------|
| OCN::SSM-ST4, page 2-115                |
| OCN::SSM-STU, page 2-115                |
| OCN::SSM-TNC, page 2-116                |
| OCN::SYNC-FREQ, page 2-118              |
| OCN::WKSWPR, page 2-127                 |
| OCN::WTR, page 2-127                    |
| STSMON::AIS-P, page 2-16                |
| STSMON::AUTOSW-AIS, page 2-25           |
| STSMON::AUTOSW-LOP (STSMON), page 2-25  |
| STSMON::AUTOSW-PDI, page 2-26           |
| STSMON::AUTOSW-SDBER, page 2-26         |
| STSMON::AUTOSW-SFBER, page 2-26         |
| STSMON::AUTOSW-UNEQ (STSMON), page 2-27 |
| STSMON::CONCAT, page 2-35               |
| STSMON::FAILTOSW-PATH, page 2-51        |
| STSMON::FORCED-REQ, page 2-65           |
| STSMON::LOCKOUT-REQ, page 2-72          |
| STSMON::LOP-P, page 2-76                |
| STSMON::MAN-REQ, page 2-87              |
| STSMON::PDI-P, page 2-94                |
| STSMON::PLM-P, page 2-96                |
| STSMON::RFI-P, page 2-102               |
| STSMON::SD-P, page 2-106                |
| STSMON::SF-P, page 2-108                |
| STSMON::TIM-P, page 2-121               |
| STSMON::UNEQ-P, page 2-124              |
| STSMON::WKSWPR, page 2-127              |
| STSTERM::AIS-P, page 2-16               |
| STSTERM::PDI-P, page 2-94               |
| STSTERM::PLM-P, page 2-96               |
| STSTERM::RFI-P, page 2-102              |
| STSTERM::SD-P, page 2-106               |
| STSTERM::SF-P, page 2-108               |
| STSTERM::TIM-P, page 2-121              |
| STSTERM::UNEQ-P, page 2-124             |
| VT-MON::AIS-V, page 2-17                |
| VT-MON::AUTOSW-AIS, page 2-25           |

**Table 2-6 Alarm Index by Alarm Type (continued)**

|                                         |
|-----------------------------------------|
| VT-MON::AUTOSW-LOP (VT-MON), page 2-26  |
| VT-MON::AUTOSW-UNEQ (VT-MON), page 2-27 |
| VT-MON::FORCED-REQ, page 2-65           |
| VT-MON::LOCKOUT-REQ, page 2-72          |
| VT-MON::LOP-V, page 2-77                |
| VT-MON::MAN-REQ, page 2-87              |
| VT-MON::UNEQ-V, page 2-125              |
| VT-MON::WKSWPR, page 2-127              |
| VT-TERM::AIS-V, page 2-17               |
| VT-TERM::PLM-V, page 2-98               |
| VT-TERM::RFI-V, page 2-103              |
| VT-TERM::SD-P, page 2-106               |
| VT-TERM::SF-P, page 2-108               |
| VT-TERM::UNEQ-V, page 2-125             |

## 2.3.1 Alarm Type/Object Definition

The following table defines abbreviations used in the alarm troubleshooting procedures.

**Table 2-7 Alarm Type/Object Definition**

|                 |                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AIP</b>      | Auxiliary interface protection module                                                                                                                                 |
| <b>BITS</b>     | Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)                                                                                        |
| <b>BPLANE</b>   | The backplane                                                                                                                                                         |
| <b>DS1</b>      | A DS1 line on a DS1 or DS3XM card                                                                                                                                     |
| <b>DS3</b>      | A DS3 line on a DS3 or DS3XM card                                                                                                                                     |
| <b>ETHER</b>    | Ethernet, such as for straight-through (CAT-5) LAN cables                                                                                                             |
| <b>ECN</b>      | An EC1 line on an EC1 card                                                                                                                                            |
| <b>EC1-12</b>   | An EC1 line on an EC1 card                                                                                                                                            |
| <b>ENV</b>      | An environmental alarm port on an AIC card                                                                                                                            |
| <b>EQPT</b>     | 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 |
| <b>EXTSYNCH</b> | BITS outgoing references (SYNC-BITS1, SYNC-BITS2)                                                                                                                     |
| <b>E1000F</b>   | An Ethernet line on an E1000 card                                                                                                                                     |
| <b>E100T</b>    | An Ethernet line on an E100 card                                                                                                                                      |
| <b>FAN</b>      | Fan-tray assembly                                                                                                                                                     |
| <b>HDGE</b>     | High Density Gigabit Ethernet. Applies to G1000 cards.                                                                                                                |
| <b>NE</b>       | The entire network element (SYSTEM)                                                                                                                                   |
| <b>NERING</b>   | Represents the ring status in the NE                                                                                                                                  |

**Table 2-7 Alarm Type/Object Definition (continued)**

|                 |                                                                      |
|-----------------|----------------------------------------------------------------------|
| <b>NE-SYNCH</b> | Represents the timing status of the NE                               |
| <b>OCN</b>      | An OCN line on an OCN card                                           |
| <b>STSMON</b>   | STS alarm detection at the monitor point (upstream of cross-connect) |
| <b>STSRNG</b>   | BLSR ring number (STSRNG)                                            |
| <b>STSTERM</b>  | STS alarm detection at termination (downstream of cross-connect)     |
| <b>VT-MON</b>   | VT1 alarm detection at the monitor point (upstream of cross-connect) |
| <b>VT-TERM</b>  | VT1 alarm detection at termination (downstream of cross-connect)     |

## 2.4 Trouble Notifications

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 reports both alarmed trouble notifications, in the Alarms tab, and non-alarmed (NA) trouble notifications, in 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 Secondary Timing Reference ([SWTOSEC](#)) or a User-Initiated Manual Reset ([MANRESET](#)) condition.

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](#)) 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. The missing cable or lost signal 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.

### 2.4.1 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 tab 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 in TL1 and in the History tab of CTC. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

### 2.4.2 Severities

The ONS 15454 uses Telcordia-standard severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service affecting alarm that needs immediate correction. Major is 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 an 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 effect 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 troubleshoot, but a minor alarm should not immediately disrupt service.

Telcordia standard severities are the default settings for the ONS 15454. You can customize ONS 15454 alarm severities with the alarm profiles feature. For alarm profile procedures, refer to the *Cisco ONS 15454 Procedure Guide*.

## 2.5 Safety Summary

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

**Caution**

---

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

---

Some troubleshooting procedures require installation or removal of optical (OC-N) cards, in these instances users should pay close attention to the following warnings:

**Warning**

---

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

---

**Warning**

---

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

---

**Warning**

---

**Class 1 laser product.**

---

**Warning**

---

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

---

## 2.6 Alarm Procedures

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

## 2.6.1 AIS

- Not Reported (NR) (Condition)

The ONS 15454 detects an Alarm Indication Signal (AIS) in the SONET overhead. The AIS condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but the DS-3 or 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

- 
- |               |                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports.                                                                                                     |
| <b>Step 2</b> | Clear the upstream alarms using the applicable procedure(s) in this chapter.                                                                                                                    |
| <b>Step 3</b> | If the condition does not clear, log on to <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a> for more information or call the Cisco Technical Assistance Center (1-800-553-2447). |
- 

## 2.6.2 AIS-L

- Not Reported (NR) (Condition)

The Alarm Indication Signal–Line condition means there is an error in the SONET overhead at the line layer. The AIS-L condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but a node upstream on the circuit does not have its 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.

The SONET 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

- 
- |               |                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Check upstream nodes and equipment for alarms, especially for LOS and an out-of-service port.                                                                                                   |
| <b>Step 2</b> | Clear the upstream alarms using the applicable procedure(s) in this chapter.                                                                                                                    |
| <b>Step 3</b> | If the condition does not clear, log on to <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a> for more information or call the Cisco Technical Assistance Center (1-800-553-2447). |
- 

## 2.6.3 AIS-P

- Not Reported (NR) (Condition)

The Alarm Indication Signal–Path condition means there is an error in the SONET overhead at the path layer. The AIS-P condition 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 an 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. The path layer 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 using the applicable procedure(s) in this chapter.
- Step 3** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.4 AIS-V

- Not Reported (NR) (Condition)

The Alarm Indication Signal–Virtual Tributary (VT) condition means there is an error in the SONET overhead at the VT layer. The AIS-V condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an 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 VT, or electrical, layer. The VT layer is created when the SONET signal is broken down into an electrical signal, for example when an optical signal enters an ONS 15454 OC-N card. If the 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 1-65.



### Note

In non-revertive UPSR configurations, VT-layer alarms or conditions (ending in \*-V) are not reported when a switch occurs due to VT-level errors. Only [WKSWPR](#) is reported.

## Procedure: Clear the AIS-V Condition

- 
- Step 1** Check upstream nodes and equipment for alarms, especially LOS and out-of-service ports.
  - Step 2** Clear the upstream alarms using the applicable procedure(s) in this chapter.
  - Step 3** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.5 APSB

- Minor (MN), Non-Service Affecting

The Automatic Protection Switching (APS) Channel Byte Failure alarm occurs when line terminating equipment detects protection switching byte failure in the incoming APS signal. The failure occurs 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** Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes.  
  
For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment may not interoperate effectively with the ONS 15454.
  - Step 2** If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you may need to replace the upstream cards for protection switching to operate properly.



### Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- 
- Step 3** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.6 APSCDFLTK

- Minor (MN), Non-Service Affecting

The APS 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.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for [BLSROSYNC](#).

## Procedure: Clear the APSCDFLTK Alarm

- 
- Step 1** Use the [“Identify a Ring ID or Node ID Number” procedure on page 2-129](#) to verify that each node has a unique node ID number.
- Step 2** Repeat [Step 1](#) for all nodes in the ring.
- If two nodes have the same node ID number, complete the [“Change a Node ID Number” procedure on page 2-129](#) to change one node’s ID number so that each node ID is unique.
- Step 3** If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the [“E-W-MISMATCH” section on page 2-47](#).) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 Procedure Guide* provides a procedure for fiberizing BLSRs.
- Step 4** If the alarm does not clear and 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 a working fiber is incorrectly attached to a protection fiber.
- Step 5** If the alarm does not clear, Use the [“Verify Node Visibility for Other Nodes” procedure on page 2-130](#) to check the ring in network view and verify that each node is visible to the other nodes.
- Step 6** If nodes are not visible, complete the [“Check or Create Node SDCC Terminations” procedure on page 2-130](#) to ensure that SDCC terminations exist on each node.
- Step 7** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.7 APSC-IMP

- Minor (MN), Non-Service Affecting

An Improper SONET Automatic Protect Switch code alarm indicates invalid K bytes. The APSC-IMP 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** Use an optical test set to determine the validity of the K byte signal by examining the received signal. For specific procedures to use the test set equipment, consult the manufacturer.
- If the K byte is invalid, the problem lies in upstream equipment and not in the reporting ONS 15454. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454s, consult the appropriate user documentation.

- 
- Step 2** If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs. Complete the “[Identify a Ring ID or Node ID Number](#)” procedure on page 2-129.
  - Step 3** Repeat [Step 2](#) for all nodes in the ring.
  - Step 4** If a node has a ring ID number that does not match the other nodes, make the ring ID number of that node identical to the other nodes. Complete the “[Change a Ring ID Number](#)” procedure on page 2-129.
  - Step 5** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.8 APSCINCON

- Minor (MN), Service Affecting

An APS–Inconsistent alarm means an inconsistent APS byte 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 APSCINCON 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).
- 

## 2.6.9 APSCM

- Major (MJ), 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

---

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

---

**Warning**

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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 are physically connected directly to the adjoining node's working-card channel fibers.
- Step 2** If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node's protection-card channel fibers.
- Step 3** If the alarm does not clear, log 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).

## 2.6.10 APSCNMIS

- Major (MJ), 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. The APSCNMIS alarm may occur and clear when a BLSR is being provisioned. If so, you can disregard the temporary occurrence. If the APSCNMIS remains raised, the alarm clears when a K byte with a valid source node ID is received.

## Procedure: Clear the APSCNMIS Alarm

- Step 1** Use the [“Identify a Ring ID or Node ID Number” procedure on page 2-129](#) to verify that each node has a unique node ID number.
- Step 2** If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.
- Step 3** Click **Close** on the Ring Map dialog box.
- Step 4** If two nodes have the same node ID number, complete the [“Change a Node ID Number” procedure on page 2-129](#) to change one node's ID number so that each node ID is unique.

**Note**

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




---

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

---

- Step 5** If the alarm does not clear, use the “[Lock Out a BLSR Span](#)” procedure on page 2-130 to lock out the span.
- Step 6** Use the “[Clear a BLSR Span Command](#)” procedure on page 2-130 to clear the lockout.
- Step 7** If the alarm 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).
- 

## 2.6.11 APSMM

- Minor (MN), Non-Service Affecting

An APS Mode Mismatch failure alarm 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. The APSMM alarm occurs in a 1+1 configuration.

### Procedure: Clear the APSMM Alarm

- 
- Step 1** For the reporting ONS 15454, display the CTC node (default login) view and check the protection scheme provisioning.
- Click the **Provisioning > Protection** tabs.
  - Choose the 1+1 protection group configured for the OC-N cards.  
The chosen protection group is the protection group optically connected (with DCC connectivity) to the far end.  
Record whether the Bidirectional Switching checkbox is checked.
- Step 2** Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned about is the protection group optically connected (with DCC connectivity) to the near end.
- Step 3** Verify that the Bidirectional Switching checkbox matches the checked or unchecked condition of the box recorded in If not, change it to match.
- Step 4** Click **Apply**.
- Step 5** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.12 AS-CMD

- Not Alarmed (NA) (Condition)



The Alarms Suppressed by User Command condition applies to the Network Element (NE), backplane, and cards. It occurs when alarms are suppressed for one or more cards or for the entire shelf.

## Procedure: Clear the AS-CMD Condition

- 
- Step 1** Click the **Conditions** tab. From the Object column and Eqpt Type column, note what entity the condition is reported against, such as against a port, slot, shelf, or against the ONS 15454.
- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and go to [Step 2](#).
- If the condition is reported against the backplane, go to [Step 6](#).
- If the Condition tab says that the object is “system,” it means that it applies to the shelf. Go to [Step 7](#).
- Step 2** If the AS-CMD condition is reported for a card, determine whether alarms are suppressed for a port and if so, raise the suppressed alarms.
- Double-click the card to display the card view.
  - Click the **Provisioning > Alarm Behavior** tabs.
    - If the Suppress Alarms column checkbox is checked for a port row, click it to deselect it and click **Apply**.
    - If the Suppress Alarms column checkbox is not checked for a port row, from the View menu, choose Go to parent view.
- Step 3** In the CTC node (default login) view, if the AS-CMD condition is reported for a card and not an individual port, click the **Provisioning > Alarm Behavior** tabs.
- Step 4** Locate the row for the reported card slot. (The slot number information was in the Object column in the **Conditions** tab that you noted in Step 1.)
- Step 5** Click the Suppress Alarms column checkbox to deselect the option for the card row.
- Step 6** If the condition is reported for the backplane, the alarms are suppressed for cards such as the AIP that are not in the optical or electrical slots.
- In the CTC node (default login) view, click the **Provisioning > Alarm Behavior** tabs.
  - In the Backplane row, click the Suppress Alarms column checkbox to deselect it and click **Apply**.
- Step 7** If the condition is reported for the shelf, cards and other equipment are affected.
- In the CTC node (default login) view, click the **Provisioning > Alarm Behavior** tabs.
  - Click the **Suppress Alarms** checkbox located at the bottom of the tab to deselect the option.
  - Click **Apply**.
- Step 8** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.13 AS-MT

- Not Alarmed (NA) (Condition)

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

To clear the AS-MT condition, complete the [“Clear a Loopback” procedure on page 2-132](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.14 AUTOLSROFF

- Critical, Service Affecting

The Auto Laser Shutdown alarm raises when the OC-192 card temperature exceeds 90 degrees Celsius. The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.



Warning

---

**On the 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 AUTOLSROFF Alarm

- 
- Step 1** View the temperature displayed on the ONS 15454 LCD front panel on the upper-right corner. For an illustration of the LCD panel, refer to NTP-70, “View Alarm Counts on the LCD for a Slot or Port,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** If the temperature of the ONS 15454 exceeds 90 degrees Celsius, the alarm should clear if you solve the ONS 15454 temperature problem. Complete the [“HITEMP” procedure on page 2-67](#).
- Step 3** If the temperature of the ONS 15454 is below 90 degrees Celsius, the ONS 15454 temperature is not the cause of the alarm, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the OC-192 card.



Note

---

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

---

- Step 4** If card replacement does not clear the alarm, 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.
-

## 2.6.15 AUTORESET

- Minor (MN), Non-Service Affecting

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

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located at 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, complete the [“Physically Replace a Card” procedure on page 2-134](#).

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

**Step 3** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.16 AUTOSW-AIS

- Not Reported (NR) (Condition)

The Automatic UPSR Switch Caused by AIS condition 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.

To clear the condition, see the [“AIS” section on page 2-16](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.17 AUTOSW-LOP (STSMON)

- Not Alarmed (Condition)

The Automatic UPSR Switch Caused by Loss of Pointer (LOP) condition 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.

To clear the condition, see the “[LOP-P](#)” section on page 2-76. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.18 AUTOSW-LOP (VT-MON)

- Minor (MN), Service Affecting

The AUTOSW-LOP alarm 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.

To clear the alarm, see the “[LOP-P](#)” section on page 2-76. If the alarm 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).

## 2.6.19 AUTOSW-PDI

- Not Alarmed (Condition)

The Automatic UPSR Switch Caused by Payload Defect Indication (PDI) condition 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.

To clear the condition, see the “[PDI-P](#)” section on page 2-94. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.20 AUTOSW-SDBER

- Not Alarmed (NA) (Condition)

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

To clear the condition, see the “[CLDRESTART](#)” section on page 2-33. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.21 AUTOSW-SFBER

- Not Alarmed (NA) (Condition)

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

To clear the condition, see the “[SF-L](#)” section on page 2-107. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.22 AUTOSW-UNEQ (STSMON)

- Not Alarmed (NA) (Condition)

The Automatic UPSR Switch Caused by Unequipped (UNEQ) condition indicates that an UNEQ alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears.

To clear the condition, see the “UNEQ-P” section on page 2-124. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.23 AUTOSW-UNEQ (VT-MON)

- Minor (MN), Service Affecting

AUTOSW-UNEQ indicates that a UNEQ alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears.

To clear the alarm, see the “UNEQ-P” section on page 2-124. If the alarm 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).

## 2.6.24 BKUPMEMP

- Critical, Non-Service Affecting

The Primary Non-Volatile Backup Memory Failure 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. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card.

### 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** If both TCC+ cards are powered and enabled, reset the active TCC+ card to make the standby TCC+ card active. Complete the “[Reset the Active TCC+ Card in CTC](#)” procedure on page 2-133.  
Wait ten minutes to verify that the card you reset completely reboots and displays as Standby. If not, call the Cisco Technical Assistance Center (1-800-553-2447).

- Step 3** If the alarm has not cleared, call the Cisco Technical Assistance Center (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
- 

## 2.6.25 BLSROSYNC

- Major (MJ), Service Affecting

The BLSR Out Of Sync alarm is caused when a node on a working ring loses its DCC connection because all transmit and receive fiber is removed, and you attempt to add or delete a circuit. The CTC cannot generate the table and raises the BLSROSYNC alarm.

### Procedure: Clear the BLSROSYNC Alarm

- 
- Step 1** Reestablish cabling continuity to the node reporting the alarm.
- Once the DCC is established between the node and the rest of the BLSR, it will become visible to the BLSR and be able to function on the circuits.
- Step 2** If alarms are raised when the DCCs are turned on, see the [“EOC” section on page 2-44](#).
- Step 3** If the alarm 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).
- 

## 2.6.26 CARLOSS (EQPT)

- Major (MJ), Service Affecting

A Carrier Loss on the LAN–Equipment alarm occurs when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC+ card or the LAN backplane pin connection on the ONS 15454. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the ONS 15454.

### Procedure: Clear the CARLOSS Alarm

- 
- Step 1** Verify connectivity by pinging the ONS 15454 that is reporting the alarm.
- If you are using a Microsoft Windows operating system, from the Start Menu choose **Programs > Accessories > Command Prompt**.
  - If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.
  - 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 CTC.
- a. Exit from CTC.
  - b. Reopen the browser.
  - c. Log into CTC.
- Step 3** Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.
- Step 4** If the straight-through (CAT-5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 5** If you are unable to establish connectivity, change out the straight-through cable with a new known-good cable.
- Step 6** If you are unable to establish connectivity, perform standard network/LAN diagnostics. For example, trace the IP route, check cables, and check any routers between the node and CTC.
- Step 7** If the alarm 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).
- 

## 2.6.27 CARLOSS (E-Series)

- Major (MJ), Service Affecting

A Carrier Loss on the LAN–E-Series Ethernet Card alarm 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 the CARLOSS alarm are a disconnected cable, an Ethernet GBIC fiber connected to an optical card rather than an Ethernet device, 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.

The CARLOSS alarm also occurs after the restoration of a node’s database. After restoration, the alarm will clear in approximately 30 seconds after spanning tree protection (STP) reestablishes. The database restoration circumstance applies to the E-series Ethernet cards but not the G1000-4 card, because the G1000-4 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 at the lower-right outside edge of the shelf assembly.

---

### Procedure: Clear the CARLOSS Alarm

- Step 1** Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.
- Step 2** If the straight-through (CAT-5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** If no misconnection to an OC-N card exists, check that the transmitting device is operational. If not, troubleshoot the device.

- Step 4** If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the straight-through (CAT-5) LAN cable connecting the transmitting device to the Ethernet port.
- Step 6** If a valid Ethernet signal is present, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the Ethernet card.
- Step 7** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the Ethernet card.

**Caution**


---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

**Note**


---

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

---

- Step 8** If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.
- An 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.
- Step 9** 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, the following steps do not apply.
- 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 network, determine the ONS 15454 and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.
    - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
    - Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
    - Click the **Circuits** tab.
    - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit will connect the Ethernet card to an OC-N card on the same node.
  - e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.
 

If one of the circuit sizes is incorrect, complete the [“Delete a Circuit” procedure on page 2-132](#).
  - f. Reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.



- Step 10** If the alarm 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).
- 

## 2.6.28 CARLOSS (G1000-4)

- Major, Service affecting

A Carrier Loss on the LAN-G-Series Ethernet Card alarm 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 is caused by one of two situations:

If the G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The LOS may be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.

If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting 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 clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as TPTFAIL or OC-N alarms or conditions on the end-to-end path will normally accompanied it.

Refer to the *Cisco ONS 15454 Reference Guide* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the [“TPTFAIL” section on page 2-122](#) for more information about 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 at the lower-right outside edge of the shelf assembly.

---

## Procedure: Clear the CARLOSS Alarm

- 
- Step 1** Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.
- Step 2** If the straight-through (CAT-5) LAN cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** If no misconnection to the OC-N card exists, check that the transmitting attached Ethernet device is operational. If not, troubleshoot the device.
- Step 4** If the alarm does not clear, use an Ethernet test set to determine that a valid signal is coming into the Ethernet port.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the straight-through (CAT-5) LAN cable connecting the transmitting device to the Ethernet port.

- Step 6** If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the G1000-4 will turn off its transmitter laser and report a CARLOSS alarm. If link autonegotiation has been enabled for the port, check for conditions which could cause autonegotiation to fail.
- Confirm that the attached Ethernet device has autonegotiation 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 previous attempts fail, disable and reenble the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process will restart.)
- Step 8** If the alarm does not clear and a TPTFAIL alarm is also reported, complete the [“TPTFAIL” procedure on page 2-122](#). If the TPTFAIL alarm is not reported, continue to the next step.




---

**Note** When the CARLOSS and the TPTFAIL 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** If the TPTFAIL alarm was not reported, check to see whether terminal loopback has been provisioned on the port.
- In the node (default login) view, click the card to go to card view.
  - Clicking the **Conditions** tab and the **Retrieve Conditions** button.
  - If LPBKTERMINAL is listed for the port, a loopback is provisioned. Go to [Step 10](#). If IS is listed, go to [Step 11](#).
- Step 10** If a loopback was provisioned, complete the [“Clear a Loopback” procedure on page 2-132](#).  
On the G1000-4 card, provisioning a terminal loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could cause the CARLOSS alarm detected by the G1000-4 port in loopback.  
If the does not have a LPBKTERMINAL condition, continue to [Step 11](#).
- Step 11** If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect. 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 setup of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, the following steps do not apply.




---

**Note** An 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.

---

- Right-click anywhere on the row of the CARLOSS alarm.
- Right-click or left-click the **Select Affected Circuits** dialog.
- Record the information in the type and size columns of the highlighted circuit.
- From the examination of the layout of your network, determine the ONS 15454 and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.
  - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.

- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
  - Click the **Circuits** tab.
  - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit will connect the Ethernet card to an OC-N card on the same node.
- e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
- If one of the circuit sizes is incorrect, complete the [“Delete a Circuit” procedure on page 2-132](#).
- f. Reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures about how to create circuits.
- Step 12** If a valid Ethernet signal is present, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#).
- Step 13** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the Ethernet card.

**Caution**


---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

**Note**


---

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

---

- Step 14** If the alarm does not clear, log 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).
- 

## 2.6.29 CLDRESTART

- Not Alarmed (NA) (Condition)

The Cold Restart condition occurs when a card is cold-restarted by being physically removed and inserted, replaced, or when the ONS 15454 is powered on.

**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 CLDRESTART Condition

- Step 1** If the condition fails to clear after the card reboots, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#).
- Step 2** If the condition does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

**Step 3** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.30 COMIOXC

- Critical, Service Affecting

The I/O Slot To Cross-Connect (XCON) Communication Failure alarm is raised by the cross-connect card. It occurs when there is a communication failure for a particular I/O slot.

### Procedure: Clear the COMIOXC Condition

- Step 1** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) on the reporting cross-connect card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 2** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 3** If the CTC reset does not clear the alarm, move traffic off the cross-connect card. Complete the [“Side Switch the Active or Standby Cross-Connect Card” procedure on page 2-131](#).
- Step 4** Complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the cross-connect card.
- Step 5** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the 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 6** If the alarm 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).
- 

## 2.6.31 CONCAT

- Critical, Service Affecting

The STS Concatenation Error alarm occurs when the transmitted STSc circuit is different from 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 the CONCAT alarm, it is more likely that the provisioned circuit size is incorrect. If an existing circuit has operated correctly 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.
- In the network view, click the **Circuits** tab.
  - Find the appropriate row using the Circuit Name and record the size listed in the size column.
  - 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, complete the [“Delete a Circuit” procedure on page 2-132](#).
- Step 3** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures about how to create circuits.
- Step 4** Check that the size of the circuit source matches the correct circuit size.
- Measuring the source signal with an optical test set to determine whether the circuit size matches the provisioned circuit.  
For specific procedures to use the test set equipment, consult the manufacturer.
  - If the source of the circuit signal is an optical test set, check that the optical test set settings match the intended circuit size.
  - If the source of the circuit signal is not an optical test set, troubleshoot the source of the circuit signal.
- Step 5** If the source of the circuit signal is an ONS 15454 or other Cisco device, 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).
- 

## 2.6.32 CONTBUS-A-18

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

A Communication Failure from TCC+ Slot to TCC+ Slot alarm occurs when the main processor on the TCC+ card in Slot 7 (termed TCC A) loses communication with the coprocessor on the same card.

**Caution**

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

## Clear the CONTBUS-A-18 Alarm

- 
- Step 1** Complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#) to make the TCC+ in Slot 11 active.
- Step 2** Wait approximately 10 minutes for the TCC+ in Slot 7 to reset as the standby TCC+. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 3** Position the cursor over the TCC+ card in Slot 11 and complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#) to make the standby TCC+ in Slot 7 active.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
- 

## 2.6.33 CONTBUS-B-18

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

A Communication Failure from TCC+ Slot to TCC+ Slot alarm occurs when the main processor on the TCC+ card in Slot 11 (termed TCC B) loses communication with the coprocessor on the same card.

**Caution**

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

## Clear the CONTBUS-B-18 Alarm

- 
- Step 1** Position the cursor over the TCC+ card in Slot 11 and complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#) to make the TCC+ in Slot 7 active.
- Step 2** Wait approximately 10 minutes for the TCC+ in Slot 11 to reset as the standby TCC+. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 3** Position the cursor over the TCC+ card in Slot 7 and complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#) to make the standby TCC+ in Slot 11 active.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
-

## 2.6.34 CONTBUS-IO-A

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

A TCC A to Shelf Slot Communication Failure alarm occurs when the active TCC+ card in Slot 7 (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm might appear briefly when the ONS 15454 switches to the protect TCC+ card. In the case of a TCC+ protection switch, the alarm clears after the other cards establish communication with the new active TCC+ card. If the alarm persists, the problem is with the physical path of communication from the TCC+ card to the reporting card. The physical path of communication includes the TCC+ card, the other card, 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 at the lower-right outside edge of the shelf assembly.

### Clear the CONTBUS-IO-A Alarm

- 
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [MEA \(Bplane\) alarm \(see page 2-89\)](#) for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby TCC+ in Slot 11, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#). Verify that the following LED behavior takes place:
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 3** If the alarm object is the standby TCC+ in Slot 11, perform a soft reset of this card:
- a. Right-click the Slot 11 TCC+ card.
  - b. Choose **Reset Card** from the shortcut menu.
  - c. Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 4** If CONTBUS-IO-A is raised on several cards at once, complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#).
- Wait ten minutes to verify that the card you reset completely reboots. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 5** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the reporting card.
- Step 6** If the reseated card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
-

## 2.6.35 CONTBUS-IO-B

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

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

The CONTBUS-IO-B alarm might appear briefly when the ONS 15454 switches to the protect TCC+ card. In the case of a TCC+ protection switch, the alarm clears after the other cards establish communication with the new active TCC+ card. If the alarm persists, the problem is with the physical path of communication from the TCC+ card to the reporting card. The physical path of communication includes the TCC+ card, the other card, 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 at the lower-right outside edge of the shelf assembly.

## Clear the CONTBUS-IO-B Alarm

- 
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [MEA \(Bplane\) alarm](#) (see page 2-89) for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby TCC+ in Slot 7, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure](#) on page 2-133. Verify that the following LED behavior takes place:
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC..
- Step 3** If the alarm object is the standby TCC+ in Slot 7, perform a soft reset of this card:
- a. Right-click the Slot 7 TCC+ card.
  - b. Choose **Reset Card** from the shortcut menu.
  - c. Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 4** If CONTBUS-IO-B is raised on several cards at once, complete the [“Reset the Active TCC+ Card in CTC” procedure](#) on page 2-133.
- Wait ten minutes to verify that the card you reset completely reboots. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 5** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure](#) on page 2-134 for the reporting card.
- Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure](#) on page 3-4. If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure](#) on page 2-134.
-



## 2.6.36 CTNEQPT-PBPROT

- Critical, Service Affecting

The Interconnection Equipment Failure–Protect Cross-Connect Card (XC) Payload Bus Alarm indicates a failure of the main payload between the protect cross-connect card (XC/XCVT/XC10G) 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 CTNEQPT-PBPROT alarm, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#) for the standby TCC+ card. If the reseat fails to clear the alarm, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the standby TCC+ card. Do not physically reseat an active TCC+ card. Reseating the TCC+ disrupts traffic.



### Caution

It can take up to 30 minutes for software to be updated on a standby TCC+ card.




### Caution

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

## Procedure: Clear the CTNEQPT-PBPROT Alarm

- Step 1** Perform a CTC reset on the standby cross-connect card (XC/XCVT/XC10G). Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#).
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 2** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- If the cross-connect reset is not complete and error-free or if the TCC+ reboots automatically, call the Cisco Technical Assistance Center (1-800-553-2447).
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the standby cross-connect card.
- Step 4** Determine whether the card is an active card in a protection group. Refer to DLP 189, “Verify that a 1+1 Working Slot is Active,” for information.
- Step 5** If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the [“Move Protection Group Traffic with a Switch Command” procedure on page 2-131](#).
- Step 6** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) on the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

- Step 7** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 8** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the reporting card.
- Step 9** Complete the [“Clear a Protection Group Switch Command” procedure on page 2-132](#).
- Step 10** If the reporting traffic card is a protect card, complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 11** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 12** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the reporting card.
- Step 13** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for 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 14** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the reporting traffic card.
- Step 15** If the alarm 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).

## 2.6.37 CTNEQPT-PBWORK

- Critical, Service Affecting

The Interconnection Equipment Failure–Working Cross-Connect Card (XC) Payload Bus alarm indicates a failure in the main payload bus between the active cross-connect card (XC/XCVT/XC10G) 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 CTNEEQPT-PBWORK alarm, complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#) for the active TCC+ card and then complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#) for it. If the reseat fails to clear the alarm, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the TCC+ card. Do not physically reseat an active TCC+ card; it disrupts 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 at the lower-right outside edge of the shelf assembly.

## Procedure: Clear the CTNEQPT-PBWORK Alarm

**Step 1** Complete the [“Side Switch the Active or Standby Cross-Connect Card” procedure on page 2-131](#) for the active cross-connect card.

**Note**

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

**Step 2** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) for the reporting card.

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

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

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 4** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the standby cross-connect card.

**Note**

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

**Step 5** If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the [“Move Protection Group Traffic with a Switch Command” procedure on page 2-131](#).

**Step 6** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) for the reporting card.

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

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

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 8** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the reporting card.

**Step 9** Complete the [“Clear a Protection Group Switch Command” procedure on page 2-132](#).

**Step 10** If the alarm does not clear, complete the [Physically Replace a Card, page 2-134](#) for the 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 11** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the reporting traffic card.

**Step 12** If the alarm 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).

---

## 2.6.38 DATAFLT

- Minor (MN), Non-Service Affecting

The Software Data Integrity Fault alarm occurs when the TCC+ exceeds its flash memory capacity.



### 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).

## 2.6.39 DS3-MISM

- Not Alarmed (NA) (Condition)

The DS3 Frame Format Mismatch condition 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 not 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 PROVISION 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 Condition

---

**Step 1** Display the CTC card 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 match the expected incoming signal, select the correct Line Type in the drop-down list.
- 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 an optical test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 7** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.40 EHIBATVG-A

- Major (MJ), Service Affecting

The Extreme High Voltage Battery A alarm occurs when the voltage level on battery lead A exceeds -56.7 Vdc. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains below -56.7 Vdc in the normal range for 120 seconds.

The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A. If the alarm 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).

## 2.6.41 EHIBATVG-B

- Major (MJ), Service Affecting

The Extreme High Voltage Battery B alarm occurs when the voltage level on battery lead B exceeds -56.7 Vdc. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains below -56.7 Vdc in the normal range for 120 seconds.

The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B. If the alarm 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).

## 2.6.42 ELWBATVG-A

- Major (MJ), Service Affecting

The Extreme Low Voltage Battery A alarm occurs when the voltage on battery feed A is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery A alarm occurs when the voltage on battery feed A drops below -40.5 Vdc. The alarm clears when voltage remains above -40.5 Vdc in the normal range for 120 seconds.

The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A. If the alarm 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).

## 2.6.43 ELWBATVG-B

- Major (MJ), Service Affecting

The Extreme Low Voltage Battery B alarm occurs when the voltage on battery feed B is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery B alarm occurs when the voltage on battery feed B drops below -40.5 Vdc. The alarm clears when voltage remains above -40.5 Vdc in the normal range for 120 seconds.

The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B. If the alarm 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).

## 2.6.44 EOC

- Major (MJ), Non-Service Affecting

The SONET Data Communications Channel (SDCC) Termination Failure alarm occurs when the ONS 15454 loses its data communications channel. 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**

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**



**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**



**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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, complete the LOS procedure as appropriate to resolve the alarm.
- Step 2** If the alarm does not clear, on the node reporting the alarm, check the physical connections from the cards to the fiber-optic cables that are configured to carry DCC traffic.

- Step 3** If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service ports by checking that the ACT LED on each OC-N card is illuminated.
- Step 4** If the ACT LEDs on CN-N cards are illuminated, complete the [“Check or Create Node SDCC Terminations” procedure on page 2-130](#) to verify that the DCC is provisioned for the ports at both ends of the fiber span.
- Step 5** Repeat [Step 4](#) at the adjacent nodes.
- Step 6** If DCC is provisioned for the ends of the span, verify that the OC-N port is active and in service.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.
  - If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 7** If the OC-N card is in service, use an optical test set to check for signal failures on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.




---

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

---

- Step 8** If no signal failures on terminations exist, 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 1-77](#).
- Step 9** If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to NTP-19, “Install the Fiber-Optic Cables,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 10** If fiber connectors are properly fastened and terminated, complete the [“Reset the Active TCC+ Card in CTC” procedure on page 2-133](#).
- Wait ten minutes to verify that the card you reset completely reboots and displays as Standby. If not, call the Cisco Technical Assistance Center (1-800-553-2447).
- 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 11** If the alarm has not cleared, call the Cisco Technical Assistance Center (1-800-553-2447). If the TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
- Step 12** If the TCC+ replacement does not clear the alarm, delete the problematic SDCC termination.
- Click the **Provisioning > SONET DCC** tabs.
  - Highlight the problematic SDCC termination.
  - Click **Delete**.
  - Click **Yes** at confirmation dialog box.
- Step 13** Recreate the SDCC termination.

- Step 14** Verify that both ends of the SDCC have been recreated at the optical ports.
- Step 15** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.45 EQPT

- Critical, Service Affecting

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BKUPMEMP alarm, see the “BKUPMEMP” section on page 2-27. The BKUPMEMP 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** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-133 for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 2** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 3** If the CTC reset does not clear the alarm, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-134.
- Step 4** If the physical reseat of the card fails to clear the alarm, complete the “[Physically Replace a Card](#)” procedure on page 2-134.



### Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.



### Note

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

- Step 5** If the alarm 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).



## 2.6.46 EQPT-MISS

- Critical, Service Affecting

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

**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, complete the [“Remove and Reinsert Fan Tray” procedure on page 2-134](#).
- Step 3** If no fan-tray assembly is present, obtain a fan-tray assembly and refer to NTP-7, “Install the Fan-Tray Assembly,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 4** If the alarm 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).
- 

## 2.6.47 E-W-MISMATCH

- Major (MJ), 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. If the alarm appears during the initial setup, 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 in CTC

- 
- Step 1** Log into the misconnected node. The misconnected node has both ring fibers misconnected. It is between the two nodes that have one of two ring fibers misconnected.

- Step 2** Click the **Maintenance > BLSR** tabs.
- Step 3** From the row of information for the fiber span, complete the “[Identify a Ring ID or Node ID Number](#)” procedure on page 2-129 to identify the node ID, ring ID, and the slot and port in the East Line list and West Line columns. Record about information before proceeding to [Step 4](#).
- Step 4** From the View menu, choose Go to Network View.
- Step 5** Delete and recreate the BLSR.
- Click the **Provisioning > BLSR** tabs.
  - Click the row from [Step 3](#) to select it and click **Delete**.
  - Click **Create**.
  - Fill in the ring ID and node ID from the information collected in [Step 3](#).
  - Click **Finish** in the BLSR Creation window.
- Step 6** Display the CTC node (default login) view and click the **Maintenance > BLSR** tabs.
- Step 7** Change the West Line pull-down menu to the slot/port you recorded for the East Line in [Step 3](#).
- Step 8** Change the East Line pull-down menu to the slot/port you recorded for the West Line in [Step 3](#).
- Step 9** Click **OK**.
- Step 10** If the alarm does not clear, see the “[E-W-MISMATCH](#)” section on page 2-47.
- Step 11** If the alarm 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).

## Procedure: Clear the E-W-MISMATCH Alarm with a Physical Switch

- Step 1** Diagram the ring setup, including nodes and spans, on a piece of paper or white board.
- Step 2** Display the CTC network view and label each of the nodes on the diagram with the same name that appears on the network map.
- Step 3** Right-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** Examine 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 should clear the alarm.



### Note

The above physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slot/ports as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

**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.

- Step 9** If the alarm 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).

## 2.6.48 EXCCOL

- Minor (MN), 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 and CTC may be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC+ card. The problem causing the alarm 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** If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC+ card and the network management LAN.
- Step 3** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.49 EXERCISE-RING-REQ

- Not Alarmed (NA) (Condition)

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

**Note**


---

EXERCISE-RING-REQ is a condition and not an alarm. It does not require troubleshooting.

---

## 2.6.50 EXERCISE-SPAN-REQ

- Not Alarmed (NA) (Condition)

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

**Note**


---

EXERCISE-SPAN-REQ is a condition and not an alarm. It does not require troubleshooting.

---

## 2.6.51 EXT

- Minor (MN), Non-Service Affecting

A Failure Detected External to the NE alarm is raised 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** tab to gather further information about the EXT alarm.
- Step 2** Perform your standard operating procedure for the environmental condition.
- Step 3** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.52 EXTRA-TRAF-PREEMPT

- Minor (MN), Non-Service Affecting

An Extra Traffic Preempted alarm is raised on OC-N cards in four-fiber BLSRs because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

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

- 
- Step 1** Verify the protection switch has occurred by checking the ring map.
- Step 2** If a ring switch has occurred, clear the alarm on the working system by following the appropriate alarm procedure.
- Step 3** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
-

## 2.6.53 FAILTOSW

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FAILTOSW Condition

**Step 1** Look up and troubleshoot the higher-priority alarm. Clearing the FAILTOSW 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 or OC-N card using the 1:N card protection group. The working DS-N or OC-N card is reporting an alarm, but not reporting a FAILTOSW alarm.

**Step 2** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the working electrical card. It is the working electrical card using the 1:N card protection and not reporting FAILTOSW.



**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Replacing the working electrical card reporting the higher-priority alarm will allow traffic to revert back to the working slot. The 1:N card is freed, and it can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW alarm.



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

**Step 3** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.54 FAILTOSW-PATH

- Not Alarmed (NA) (Condition)

The Fail to Switch to Protection–Path condition occurs when the working path does not switch to the protection path on a UPSR. Common causes of the FAILTOSW-PATH 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 Condition on a UPSR Configuration

**Step 1** Complete the [“Clear a UPSR Lockout” procedure on page 2-131](#) to ensure there is no lockout set.

**Step 2** If none is set, check the fiber connections to ensure they are securely fastened and intact.



**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.

**Step 3** If fiber connections are correct, ensure the OC-N cards are active and in service.

- a. Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card. A green LED indicates an Active card. A yellow LED indicates a Standby card.
- b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
- c. Click the **Provisioning > Line** tabs.
- d. Verify that the State column lists the port as IS.
- e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 4** If OC-N cards are active and in service, 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, complete the [“Move Protection Group Traffic with a Switch Command” procedure on page 2-131](#) for the reporting traffic card if it is active.

**Step 6** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-133](#) for the reporting card.

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

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

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 8** If the condition persists, complete the [Remove and Reinsert \(Reseat\) a Card, page 2-134](#) for the reporting card.

**Step 9** If the traffic does not switch, complete the [Reset a Traffic Card in CTC, page 2-133](#).

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

- Step 10** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 11** If the reset does not clear the condition, complete the [“Move Protection Group Traffic with a Switch Command” procedure on page 2-131](#) again after the protect cards have booted up completely.
- Step 12** If you are unable to perform a switch, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-134](#) for the protect card.
- Step 13** If the physical reset does not clear the condition, complete the [“Move Protection Group Traffic with a Switch Command” procedure on page 2-131](#) again.
- Step 14** Complete the [“Clear a Protection Group Switch Command” procedure on page 2-132](#).
- Step 15** If the condition does not clear, complete the [“Physically Replace a Card” procedure on page 2-134](#) for the protect card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

- Step 16** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.55 FAILTOSWR

- Not Alarmed (NA) (Condition)

The Fail to Switch to Protection–Ring condition signals an APS ring switch failure. FAILTOSWR clears when one of the following actions occurs: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as 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 Condition on a Four-Fiber BLSR Configuration

- 
- Step 1** Perform the EXERCISE RING command on the BLSR.
- Click the **Provisioning > BLSR** tabs.
  - Click the row of the affected ring under the West Switch column.
  - Select **Exercise Ring** in the drop-down list.
- Step 2** If the condition does not clear, display the CTC network view.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node and click the **Maintenance > BLSR** 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.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.
  - If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 6** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.
- Step 7** If fiber continuity to ports is ok, verify that the correct port is in service.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.
  - If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.




---

**Caution**

Using an optical 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** If the correct port is in service, use an optical test set to verify that a valid signal exists on the line.  
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 9** If the signal is valid, clean the fiber. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card’s receiver specifications. The [“Optical Card Transmit and Receive Levels” section on page 1-77](#) lists these specifications.
- Step 11** Repeat Steps 6–10 for any other ports on the card.



- Step 12** If the optical power level for all OC-N cards is within specifications, complete the “[Physically Replace a Card](#)” procedure on page 2-134 for the protect standby OC-N card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4–12 for each of the nodes in the ring.
- Step 14** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.56 FAILTOSWS

- Not Alarmed (NA) (Condition)

The Failure to Switch to Protection–Span condition 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.

To clear the condition, see the “[FAILTOSWR](#)” section on page 2-53. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.57 FAN

- Critical, Service Affecting

The Fan Failure 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 whether it needs replacement. Refer to NTP-107, “Inspect and Maintain the Air Filter,” in the *Cisco ONS 15454 Procedure Guide* for the detailed procedure.
- Step 2** If the filter is clean, complete the “[Remove and Reinsert Fan Tray](#)” procedure on page 2-134.




---

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

---

- Step 3** If the fan does not run or the alarm persists, complete the [“Replace the Fan-Tray Assembly” procedure on page 3-11](#).
- Step 4** 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).
- 

## 2.6.58 FE-AIS

- Not Alarmed (NA) (Condition)

The Far-End AIS condition occurs when the far-end node’s DS3XM-6 or DS3-12E card is reports an AIS. The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting the FE-AIS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

### Procedure: Clear the FE-AIS Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS 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 condition.
- Step 3** View and clear the main alarm. See the [“AIS” section on page 2-16](#).
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.59 FE-DS1-MULTLOS

- Not Alarmed (NA) (Condition)

The Far End Multiple DS1 LOS Detected on DS3XM-6 condition occurs when 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-MULTLOS condition. 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-DS1-MULTLOS Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE 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.
  - Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
  - Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.60 FE-DS1-NSA

- Not Alarmed (NA) (Condition)

The Far End DS1 Equipment Failure–Non-Service Affecting condition occurs when a far-end DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

### Procedure: Clear the FE-DS1-NSA Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
  - Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
  - Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.61 FE-DS1-SA

- Not Alarmed (NA) (Condition)

The Far End DS1 Equipment Failure–Service Affecting condition occurs when a far-end DS-1 equipment failure occurs and affects service because even though the port is protected, traffic is unable to switch to the protect port.

The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

### Procedure: Clear the FE-DS1-SA Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
  - Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
  - Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.62 FE-DS1-SNGLLOS

- Not Alarmed (NA) (Condition)

The Far End Single DS1 LOS on the DS3XM-6 condition occurs when one of the DS1-14 ports 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 the FE-DS1-SNGLLOS alarm. Troubleshoot the FE condition 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 condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 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.
  - Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
  - Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.63 FE-DS3-NSA

- Not Alarmed (NA) (Condition)

The Far End DS3 Equipment Failure – Non-Service Affecting condition occurs when a far-end DS-3 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE in an alarm or condition message means the main alarm is occurring at the far-end node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

### Procedure: Clear the FE-DS3-NSA Condition

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.

- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.64 FE-DS3-SA

- Not Alarmed (NA) (Condition)

The Far End DS3 Equipment Failure Service Affecting condition occurs when a far-end DS-3 equipment failure occurs and affects service because even though the port is protected, traffic is unable to switch to the protect port.

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 condition. 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-DS3-SA Condition

---

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.65 FE-EQPT-NSA

- Not Alarmed (NA) (Condition)

The Far End Common Equipment Failure condition occurs when a non-service affecting equipment failure is detected on 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 the 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 condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 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.
- Step 3** View and clear the main alarm. Refer to the appropriate alarm section for troubleshooting instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.66 FE-EXERCISING-RING

- Not Alarmed (NA) (Condition)

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



**Note**

FE-EXERCISING-RING is a condition and not an alarm. It does not require troubleshooting.

---

## 2.6.67 FE-EXERCISING-SPAN

- Not Alarmed (NA) (Condition)

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



**Note**

FE-EXERCISING-SPAN is a condition and not an alarm. It does not require troubleshooting.

---

## 2.6.68 FE-FRCDWKSWPR-RING

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-FRCDWKSWPR-RING Condition

---

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS 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 condition.

- Step 3** View and clear the main alarm. See the “[Clear a BLSR Span Command](#)” procedure on page 2-130 for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.69 FE-FRCDWKSWPR-SPAN

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-FRCDWKSWPR-SPAN Condition

---

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** View and clear the main alarm. See the “[Clear a BLSR Span Command](#)” procedure on page 2-130 for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.70 FE-IDLE

- Not Alarmed (NA) (Condition)

The Far End Idle condition occurs when 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 the FE-IDLE condition. 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 condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 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.

- Step 3** View and clear the main alarm. See the “[Clear a BLSR Span Command](#)” procedure on page 2-130 for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.71 FE-LOCKOUTOFPR-SPAN

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-LOCKOUTOFPR-SPAN Condition

---

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** Make sure there is no lockout set. See the “[Clear a BLSR Span Command](#)” procedure on page 2-130 for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.72 FE-LOF

- Not Alarmed (NA) (Condition)

The Far End LOF condition occurs when 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 the FE-LOF condition. 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 condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 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.
- Step 3** View and clear the main alarm. See the “[LOF \(DS3\)](#)” section on page 2-74 for instructions.



- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.73 FE-LOS

- Not Alarmed (NA) (Condition)

The Far End LOS condition occurs when a far-end node reports a DS-3 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 the FE-LOS condition. Troubleshoot the FE condition 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 condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 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.
- Step 3** View and clear the main alarm. See the [“LOS \(DS-3\)” section on page 2-80](#) for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.74 FE-MANWKSWPR-RING

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-MANWKSWPR-RING Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** View and clear the main alarm. See the [“Clear a BLSR Span Command” procedure on page 2-130](#) for instructions.

- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.75 FE-MANWKSWPR-SPAN

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-MANWKSWPR-SPAN Condition

- 
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an 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 condition.
- Step 3** View and clear the main alarm. See the [“Clear a BLSR Span Command” procedure on page 2-130](#) for instructions.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.76 FEPRLF

- Minor (MN), Non-Service Affecting

The Far End Protection Line Failure alarm occurs when an APS switching channel signal failure occurs 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 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.
- Step 3** View and clear the main alarm. Refer to the appropriate alarm section for instructions.

- Step 4** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.77 FORCED-REQ

- Not Alarmed (NA) (Condition)

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

To clear the condition, complete the “[Clear a BLSR Span Command](#)” procedure on page 2-130. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.78 FORCED-REQ-RING

- Not Alarmed (NA) (Condition)

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

To clear the condition, see the “[FORCED-REQ](#)” section on page 2-65. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.79 FORCED-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Force Switch Request–Span condition applies to optical line cards when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

To clear the condition, see the “[FORCED-REQ](#)” section on page 2-65. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.80 FRCDSWTOINT

- Not Alarmed (NA) (Condition)

The Force Switch to Internal Timing condition occurs when the user issues a forced switch command to switch to Internal timing.

**Note**

FRCDSWTOINT is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.81 FRCDSWTOPRI

- Not Alarmed (NA) (Condition)

The Force Switch to Primary Timing Source condition occurs when the user issues a forced switch command to switch to the primary timing source.



**Note**

FRCDSWTOPRI is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.82 FRCDSWTOSEC

- Not Alarmed (NA) (Condition)

The Force Switch to Second Timing Source condition occurs when the user issues a forced switch command to switch to the second timing source.



**Note**

FRCDSWTOSEC is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.83 FRCDSWTOTHIRD

- Not Alarmed (NA) (Condition)

The Force Switch to Third Timing Source condition occurs when the user issues a forced switch command to switch to the third timing source.



**Note**

FRCDSWTOTHIRD is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.84 FRNGSYNC

- Major (MJ), Service Affecting

The Free Running Synchronization Mode alarm occurs when the reporting ONS 15454 is in free run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the 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 the FRNGSYNC 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** If the BITS source is valid, view and clear alarms related to the failures of the primary and secondary reference sources, such as the “[SYNCPRI](#)” section on page 2-119 and the “[SYNCSEC](#)” section on page 2-119.
- Step 4** If the alarm 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).
- 

## 2.6.85 FSTSYNC

- Minor (MN), 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.

The FSTSYNC alarm disappears after approximately 30 seconds. If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

**Note**

---

FSTSYNC is an informational alarm and does not require troubleshooting.

---

## 2.6.86 FULLPASSTHR-BI

- Not Alarmed (NA) (Condition)

The Bidirectional Full Pass-Through Active condition is raised on a non-switching node for a BLSR ring when the protect channels on the node are active and carrying traffic, and there is a change in the receive K byte from No Request.

To clear the condition, complete the “[Clear a BLSR Span Command](#)” procedure on page 2-130. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.87 HITEMP

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

The High Temperature alarm occurs when 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** View the temperature displayed on the ONS 15454 LCD front panel on the upper-right corner. For an illustration of the LCD panel, refer to NTP-70, “View Alarm Counts on the LCD for a Slot or Port,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** Check that the environmental temperature of the room is not abnormally high.
- Step 3** If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454.
- Step 4** If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 empty slots. Blank faceplates help airflow.
- Step 5** If faceplates fill the empty slots, check the condition of the air filter to see whether it needs replacement. Refer to NTP-107, “Inspect and Maintain the Air Filter,” in the *Cisco ONS 15454 Procedure Guide* for the detailed procedure.
- Step 6** If the filter is clean, complete the [“Remove and Reinsert Fan Tray” procedure on page 2-134](#).




---

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

---

- Step 7** If the fan does not run or the alarm persists, complete the [“Replace the Fan-Tray Assembly” procedure on page 3-11](#).
- Step 8** 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) if it applies to the NE, or a non-service affecting problem if it applies to equipment.
- 

## 2.6.88 HLDOVRSYNC

- Major (MJ), Service Affecting

The Holdover Synchronization Mode alarm indicates a loss of the primary or secondary timing reference. Timing reference loss occurs when line coding on the timing input is different from the configuration on the ON 15454. It also usually occurs during the selection of a new node reference clock. The HLDOVRSYNC 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 HLDOVRSYNC Alarm

- 
- Step 1** View and clear additional alarms that relate to timing, such as [FRNGSYNC](#), [FSTSYNC](#), [HLDOVRSYNC](#), [LOF \(BITS\)](#), [LOS \(BITS\)](#), [MANSWTOINT](#), [MANSWTOPRI](#), [MANSWTOSEC](#), [MANSWTOHTRD](#), [SWTOPRI](#), [SWTOSEC](#), [SWTOHTRD](#), [SYNC-FREQ](#), [SYNCPRI](#), [SYNCSEC](#), or [SYNCTHIRD](#).
- Step 2** Reestablish a primary and secondary timing source according to local site practice.

- Step 3** If the alarm 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).

## 2.6.89 IMPROPRMVL

- Critical, Service Affecting

The Improper Removal alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm, it only needs to be recognized by CTC and the TCC+ card. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node.



**Note**

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



**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card.



**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** If the card is not in service, right-click the card reporting the IMPROPRMVL and choose **Delete**.



**Note**

CTC will not allow you to delete the reporting 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 2** 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.

- In CTC, double-click the reporting card to display the card view.
- Click the **Provisioning** tab.
- Click the **State** of any in-service ports.
- Choose **OOS** to take the ports out of service.

**Step 3** If a circuit has been mapped to the card, complete the [Delete a Circuit, page 2-132](#).




---

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

---

**Step 4** 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 5** If the card is provisioned for DCC, delete the SDCC 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 6** 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 7** Right-click the card reporting the IMPROPRMVL and choose **Delete**.

**Step 8** If the alarm 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).

---

## 2.6.90 INC-ISD

- Not Alarmed (NA) (Condition)

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting card is OOS-MNT. It is resolved when the OOS condition ends.




---

**Note** INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.91 INHSWPR

- Not Alarmed (NA) (Condition)

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



## Procedure: Clear the INHSWPR Condition

- 
- Step 1** In the CTC node (default login) view, click the **Maintenance > Protection** tabs.
  - Step 2** Under the Protection Groups column, click the group. The Selected Group column will list the status of all cards or ports in the group.
  - Step 3** Click the card or port that says LOCKED OUT.
  - Step 4** If the card or port is locked, click the **Unlock** button.
  - Step 5** If it is switched, click the **Clear** button.
  - Step 6** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.92 INHSWWKG

- Not Alarmed (NA) (Condition)

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

## Procedure: Clear the INHSWWKG Condition

- 
- Step 1** In the CTC node (default login) view, click the **Maintenance > Protection** tabs.
  - Step 2** Under the Protection Groups column, click the group. The Selected Group column will list the status of all cards or ports in the group.
  - Step 3** Click the card or port that says LOCKED OUT.
  - Step 4** If the card or port is locked, click the **Unlock** button.
  - Step 5** If it is switched, click the **Clear** button.
  - Step 6** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.93 INVMACADR

- Major (MJ), Non-Service Affecting

The Equipment Failure Invalid MAC Address alarm occurs when 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).

## 2.6.94 KB-PASSTHR

- Not Alarmed (NA) (Condition)

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

To clear the condition, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.95 LKOUTPR-S

- Not Alarmed (NA) (Condition)

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

To clear the lockout, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.96 LOCKOUT-REQ

- Not Alarmed (NA) (Condition)

The Lockout Switch Request on Facility/Equipment condition occurs when a user initiates a lockout switch request for an 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 condition.

To clear the lockout, complete the [Clear a UPSR Lockout, page 2-131](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.97 LOCKOUT-REQ-RING

- Not Alarmed (NA) (Condition)

The Lockout Switch Request–Ring condition is raised when a LOCKOUT RING command is applied to a BLSR to keep traffic locked out of either working or protect systems.

To clear the lockout, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.98 LOCKOUT-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Lockout Switch Request–Span condition is raised when a LOCKOUT SPAN command is applied to a BLSR to lock traffic out of either a working or protect span.

To clear the lockout, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.99 LOF (BITS)

- Major (MJ), Service Affecting

The Loss of Frame (LOF) alarm occurs when 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+.
- In CTC node (default login) view or card view, note the slot and port reporting the alarm.
  - Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.
  - Click the **Provisioning > Timing** tabs to display the General Timing window.
  - Verify that **Coding** matches the coding of the BITS timing source (either B8ZS or AMI).
  - If the coding does not match, click **Coding** to reveal a menu. Choose the appropriate coding.
  - Verify that **Framing** matches the framing of the BITS timing source (either ESF or SF [D4]).
  - 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+, complete the [Physically Replace a Card, page 2-134](#) for 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.

- Step 3** If the alarm 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).

## 2.6.100 LOF (DS1)

- Major (MJ), Service Affecting

The DS1 LOF 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.
- In CTC, note the slot and port reporting the alarm.
  - 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 the format information.
  - Display the card view of the reporting card.
  - Click the **Provisioning > Line** tabs.
  - Verify that the line type of the reporting port matches the line type of the signal source.
  - If the signal source line type does not match the reporting port, click **Line Type** to reveal a menu. Choose the matching type.
  - Verify that the reporting Line Coding matches the signal source's Line Type.
  - 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.

---

- Step 2** If the alarm 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).
- 

## 2.6.101 LOF (DS3)

- Critical, Service Affecting

The LOF 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.

To clear the alarm, change the line type of the non-ONS equipment attached to the reporting card to C-bit. If the alarm 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).

## 2.6.102 LOF (EC1-12)

- Critical, Service Affecting

The LOF alarm occurs when a port on the reporting EC1-12 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 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** Verify cabling continuity to the port reporting the alarm.
- Step 2** If cabling continuity is ok, clean the fiber connectors. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the alarm does not clear, see “[Network Troubleshooting Tests](#)” section on page 1-2 to isolate the fault causing the LOF alarm.
- Step 4** If the alarm does not clear, or if you need assistance in conducting network troubleshooting tests, call the Cisco Technical Assistance Center to report a service affecting problem (1-800-553-2447).
- 

## 2.6.103 LOF (OC-N)

- Critical, Service Affecting

The LOF alarm occurs when 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** Verify cabling continuity to the port reporting the alarm.
- Step 2** If cabling continuity is ok, clean the fiber connectors. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.

- Step 3** If the alarm does not clear, see the “[Network Troubleshooting Tests](#)” section on page 1-2 to isolate the fault causing the LOF alarm.
- Step 4** If the alarm does not clear, or if you need assistance in conducting network troubleshooting tests, call the Cisco Technical Assistance Center to report a service affecting problem (1-800-553-2447).

## 2.6.104 LOP-P

- Critical, Service Affecting

A Loss of Pointer alarm indicates that the pointer at the path level has been lost. 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 the LOP-P alarm is that the received payload does not match the provisioned payload. LOP-P 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** If cabling and connections are ok, complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 3** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 4** If the reset does not clear the alarm, complete the [Move Protection Group Traffic with a Switch Command, page 2-131](#).



### 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 5** Complete the [Clear a Protection Group Switch Command, page 2-132](#).
- Step 6** If the alarm does not clear, 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 7** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the far-end card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 8** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 9** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 10** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 11** Complete the [Move Protection Group Traffic with a Switch Command, page 2-131](#) for the far-end working card.



---

**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 12** Complete the [Clear a Protection Group Switch Command, page 2-132](#).
- Step 13** If the alarm does not clear, complete the [Physically Replace a Card, page 2-134](#) for the far-end card.



---

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---



---

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

---

- Step 14** If the alarm 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).
- 

## 2.6.105 LOP-V

- Major (MJ), Service Affecting

The VT LOP 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 the 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.

**Note**

In non-revertive UPSR configurations, VT-layer alarms or conditions (ending in \*-V) are not reported when a switch occurs due to VT-level errors. Only [WKSWPR](#) is reported.

## Procedure: Clear the LOP-V Alarm

- 
- Step 1** Verify the continuity of the cabling and physical connections on the reporting card.
- Step 2** If cabling and connections are ok, complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 3** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 4** If the reset does not clear the alarm, complete the [Move Protection Group Traffic with a Switch Command, page 2-131](#).

**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 5** Complete the [Clear a Protection Group Switch Command, page 2-132](#).
- Step 6** If the alarm does not clear, the problem is at the far-end node. If the Verify the cabling and physical connections that connect to the far-end card.
- Step 7** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the far-end card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 8** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.



- Step 9** Switch from the far-end working card to the far-end protect card.
- Step 10** If the alarm 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).
- 

## 2.6.106 LOS (BITS)

- Major (MJ), Service Affecting

This LOS alarm indicates the TCC+ card has an 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** If wiring is ok, check that the BITS clock is operating properly.
- Step 3** If the alarm 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).
- 

## 2.6.107 LOS (DS-1)

- Major (MJ), Service Affecting

This LOS for either a DS-3 port or a DS1-14 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** If cabling is ok, verify that the correct port is in service.
- a. Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.

- b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - c. Click the **Provisioning > Line** tabs.
  - d. Verify that the State column lists the port as IS.
  - e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 3** If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 4** If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.
- Step 5** If a valid signal exists, replace the DS-N connector on the ONS 15454.
- Step 6** Repeat Steps 1–5 for any other port on the card that reports the LOS.
- Step 7** If the alarm does not clear, look for and troubleshoot any other alarm that may identify the source of the problem.
- Step 8** If no other alarms are present that may be the source of the LOS, or if clearing such an alarm did not clear the LOS, complete the [Physically Replace a Card, page 2-134](#) for the reporting card.

**Caution**


---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

**Note**


---

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

---

- Step 9** If the alarm 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).
- 

## 2.6.108 LOS (DS-3)

- Major (MJ), Service Affecting

This LOS for either a DS-3 port or a DS1-14 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

**Caution**


---

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** If the cabling is ok, verify that the correct port is in service.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.
  - If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 3** If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line.  
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 4** If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.
- Step 5** If a valid signal exists, replace the DS-N connector on the ONS 15454.
- Step 6** Repeat Steps 1–5 for any other port on the card that reports the LOS.
- Step 7** If the alarm does not clear, look for and troubleshoot any other alarm that may identify the source of the problem.
- Step 8** If no other alarms exist that may be the source of the LOS or if clearing such an alarm did not clear the LOS, complete the [Physically Replace a Card, page 2-134](#) for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

- Step 9** If the alarm 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).

## 2.6.109 LOS (EC1-12)

- Critical, Service Affecting

This LOS alarm on an EC1-12 port 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 reporting the alarm.
- Step 2** If the cabling is ok, verify that the correct port is in service.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card. A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.
  - If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 3** If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 4** If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.
- Step 5** If a valid signal exists, replace the cable connector on the ONS 15454.
- Step 6** Repeat Steps 1–5 for any other port on the card that reports the LOS.
- Step 7** If the alarm does not clear, look for and troubleshoot any other alarm that may identify the source of the problem.
- Step 8** If no other alarms exist that may be the source of the LOS or if clearing such an alarm did not clear the LOS, complete the [Physically Replace a Card, page 2-134](#) for the reporting card.



### Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.



### Note

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

- Step 9** If the alarm 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).
- 

## 2.6.110 LOS (OC-N)

- Critical, Service Affecting

An OC-N LOS alarm 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**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).

**Warning**

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** If the cabling is ok, verify that the correct port is in service.
- a. Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card. A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - c. Click the **Provisioning > Line** tabs.
  - d. Verify that the State column lists the port as IS.
  - e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 3** If the correct port is in service, clean the fiber connectors. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 4** If the alarm does not clear, 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 1-77 lists these specifications for each card.
- Step 5** If optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.
- For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 6** If a valid signal exists, replace the connector on the backplane.
- Step 7** Repeat Steps 1–6 for any other port on the card reporting the alarm.
- Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that may identify the source of the problem.
- Step 9** If no other alarms exist that may be the source of the LOS or if clearing such an alarm did not clear the LOS, complete the [Physically Replace a Card](#), page 2-134 for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**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 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).

## 2.6.111 LPBKDS1FEAC

- Not Alarmed (NA) (Condition)

A Loopback Caused by FEAC Command DS1 condition on the DS3XM-6 card occurs when 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 [“Using the DS3XM-6 Card FEAC \(Loopback\) Functions” section on page 1-21](#).

**Caution**

The CTC permits loopbacks on an in service circuit. Loopbacks are service affecting.

**Note**

LPBKDS1FEAC is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.112 LPBKDS1FEAC-CMD

- Not Alarmed (NA) (Condition)

The DS1 Loopback Command Sent To Far End condition when is raised when a FEAC loopback code is sent to a DS1 port on a DS3XM-6 card.

**Note**

LPBKDS1FEAC-CMD is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.113 LPBKDS3FEAC

- Not Alarmed (NA) (Condition)

A Loopback Due to FEAC Command DS3 condition occurs when 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. LPBKDS3FEAC 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 [“Using the DS3XM-6 Card FEAC \(Loopback\) Functions” section on page 1-21](#).

**Caution**

---

The CTC permits loopbacks on an in-service circuit. Loopbacks are service affecting.

---

**Note**

---

LPBKDS3FEAC is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.114 LPBKDS3FEAC-CMD

- Not Alarmed (NA) (Condition)

The DS3 Loopback Command Sent To Far End condition is raised when a FEAC loopback is sent to a DS3XM-6 card.

**Note**

---

LPBKDS3FEAC-CMD is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.115 LPBKFACILITY (DS-N or EC1-12)

- Not Alarmed (NA) (Condition)

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information about loopbacks, see the [“Network Troubleshooting Tests” section on page 1-2](#) or the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-4](#).

There are three types of loopbacks: Facility, 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. Loopbacks are service affecting.

---

**Note**


---

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

---

## Procedure: Clear the L BK FACILITY Condition

- 
- Step 1** From the CTC node (default login) view, double-click the reporting card to display the card view.
- Step 2** Click the **Maintenance** tab.
- If the condition is reported against a DS3XM-6 card, also click the **DS1** tab.
- Step 3** Complete the [Clear a Loopback, page 2-132](#).
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.116 LPBK FACILITY (OC-N)

- Not Alarmed (NA) (Condition)

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or section of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network section. By setting up loopbacks on various parts of the network and excluding other parts, you can logically isolate the source of the problem. For more information about loopbacks, see the [“Identify Points of Failure on an OC-N Circuit Path” section on page 1-22](#).

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.

To clear the loopback condition, complete the [Clear a Loopback, page 2-132](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

**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.

---



## 2.6.117 LPBKTERMINAL (DS-N, EC1-12, OC-N)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a suspect link or part of the network, and a signal comes back to the sending device. If the signal does not come back or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically isolate the source of the problem. For more information about loopbacks, see the “[Network Troubleshooting Tests](#)” section on page 1-2.

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.

To clear the loopback condition, complete the [Clear a Loopback, page 2-132](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

**Note**

---

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

---

## 2.6.118 LPBKTERMINAL(G1000-4)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software terminal loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter logically isolates the source of the problem. For more information about loopbacks, see the “[Network Troubleshooting Tests](#)” section on page 1-2.

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. Loopbacks are service affecting.

To clear the loopback condition, complete the [Clear a Loopback, page 2-132](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.119 MAN-REQ

- Not Alarmed (NA) (Condition)

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

To clear the condition, complete the [Clear a UPSR Lockout, page 2-131](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.120 MANRESET

- Not Alarmed (NA) (Condition)

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the alarm. The MANRESET condition clears automatically when the card finishes resetting.



**Note**

---

MANRESET is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.121 MANSWTOINT

- Not Alarmed (NA) (Condition)

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to the internal timing source.



**Note**

---

MANSWTOINT is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.122 MANSWTOPRI

- Not Alarmed (NA) (Condition)

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary source.



**Note**

---

MANSWTOPRI is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.123 MANSWTOSEC

- Not Alarmed (NA) (Condition)

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to the second source.



**Note**

---

MANSWTOSEC is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.124 MANSWTOTHIRD

- Not Alarmed (NA) (Condition)

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the third source.

**Note**

MANSWTOTHIRD is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.125 MANUAL-REQ-RING

- Not Alarmed (NA) (Condition)

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on a two-fiber BLSR ring to switch from working to protect or protect to working.

To clear the condition, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.126 MANUAL-REQ-SPAN

- Not Alarmed (NA) (Condition)

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span, or vice versa.

To clear the condition, complete the [Clear a BLSR Span Command, page 2-130](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.127 MEA (AIP)

- Critical, Service Affecting

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the Alarm Interface Panel (AIP), the fuse in the AIP board blew or is missing. The MEA 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).

To clear the alarm, complete the [“Replace the Alarm Interface Panel” procedure on page 3-13](#). If the alarm 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).

## 2.6.128 MEA (Bplane)

- Critical (CR), Service Affecting

The MEA alarm for the backplane means that the revision of the backplane is incompatible with cross-connect (XC10G) equipment.

## Procedure: Clear the MEA Alarm

- 
- Step 1** If the MEA is also raised against other equipment, such as the AIP or a fan tray, troubleshoot these alarms first.
- Step 2** If alarms are reported directly against the XC10G card, such as [SWMTXMOD](#), troubleshoot these alarms next.
- Step 3** If the alarm does not clear, 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 node (default login) 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 4** If the shelf assembly is not compatible with 10-Gbps equipment, 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).
- 

## 2.6.129 MEA (EQPT)

- Critical, Service Affecting

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older, pre-ANSI (15454-SA-NEBS3E, hardware part number 800-08149-XX 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, hardware part number 800-19857-XX). 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 node (default login) view, click the **Inventory** tab.
- Under the Hardware Part # column, if the part number is 800-19857-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, 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 tab 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, complete the [Physically Replace a Card, page 2-134](#) for the reporting card.



**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**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 **State** of any in-service ports.
- d. Choose **OOS** to take the ports out of service.

**Step 7** If a circuit has been mapped to the card, complete the [Delete a Circuit, page 2-132](#).




---

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

---

**Step 8** If the card is paired in a protection scheme, delete the protection group.

- a. Click the **Provisioning > Protection** tabs.
- b. Choose the protection group of the reporting card.
- c. Click **Delete**.

**Step 9** Right-click the card reporting the alarm.

**Step 10** Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

**Step 11** If the alarm does not clear, log 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).

---

## 2.6.130 MEA (FAN)

- Critical, Service Affecting

The MEA 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 node (default login) 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. Obtain a newer fan-tray assembly (15454-FTA3) with a 5 Amp fuse and complete the [“Replace the Fan-Tray Assembly” procedure on page 3-11](#).
- Step 3** If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the [“Replace the Fan-Tray Assembly” procedure on page 3-11](#).
- Step 4** If the alarm 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).
- 

## 2.6.131 MEM-GONE

- Major (MJ), 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 about alarm clears. The alarm clears when additional memory becomes available.

If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.132 MEM-LOW

- Minor (MN), 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.

If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.133 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 (EEPROM). Either the memory module on the component failed or the TCC+ lost the ability to read that module. The EEPROM 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** Perform a CTC reset on the TCC+ card. Complete the [Reset the Active TCC+ Card in CTC, page 2-133](#).

Wait ten minutes to verify that the card you reset completely reboots and displays as Standby. If not, call the Cisco Technical Assistance Center (1-800-553-2447).

- Step 2** If the alarm has not cleared, call the Cisco Technical Assistance Center (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+” procedure on page 3-4](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-134](#).
- Step 3** If the MFGMEM alarm continues to report after replacing the TCC+ cards, the problem lies in the EEPROM.
- Step 4** If the MFGMEM is reported from the fan tray, obtain a fan-tray assembly and complete the [“Replace the Fan-Tray Assembly” procedure on page 3-11](#).
- Step 5** 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).
- Step 6** If the alarm 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).

## 2.6.134 PDI-P

- Not Alarmed (NA) (Condition)

A PDI Path condition indicates a signal label mismatch failure (SLMF). An invalid signal label C2 byte in the SONET path overhead causes an SLMF. The C2 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 often accompanies the PDI-P condition. If the PDI-P is the only condition reported with the AIS, clear the PDI-P condition to clear the AIS condition. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on the port of an OC-N card supporting a G1000-4 card circuit might result from the end-to-end Ethernet link integrity feature of the G1000-4. If the link integrity is the cause, it typically is accompanied by an TPTFAIL or a CARLOSS (G1000-4) reported against one or both Ethernet ports terminating the circuit. If TPTFAIL or CARLOSS are reported against one or both of the Ethernet ports, troubleshooting the accompanying alarm clears the PDI-P condition.



**Warning**

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**



**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**



**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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.
- Click the **Circuits** tab.
  - Verify that the State column lists the port as active.
  - 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, ensure that the signal source to the card reporting the alarm is working.

- Step 3** If traffic is affected, complete the [Delete a Circuit, page 2-132](#).

**Caution**

Deleting a circuit may affect traffic.

- Step 4** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures about how to create circuits.
- Step 5** If circuit deletion and recreation does not clear the condition, check the far-end OC-N card that provides STS payload to the reporting card.
- Step 6** If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.
- Step 7** If the condition does not clear, clean the far-end optical fiber. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 8** If the condition does not clear, complete the [Physically Replace a Card, page 2-134](#) for the optical/electrical cards.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

- Step 9** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.135 PEER-NORESPONSE

- Major (MJ), 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. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

### Procedure: Clear the PEER-NORESPONSE Alarm

- 
- Step 1** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 2** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 3** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 4** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 5** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.136 PLM-P

- Critical, Service Affecting

A Payload Label Mismatch–Path alarm indicates an SLMF. An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal label byte. It 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**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).


**Warning**

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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.
- Click the **Circuits** tab.
  - Verify that the State column lists the port as active.
  - 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 with an optical test set according to site specific practice.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If traffic is being affected, complete the [Delete a Circuit, page 2-132](#).
- 
-  **Caution** Deleting a circuit may affect traffic.
- 
- Step 4** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures about how to create circuits.
- Step 5** If the circuit deletion and recreation does not clear the alarm, verify the far-end OC-N card that provides STS payload to the DS-N card.
- Step 6** If the alarm does not clear, verify the cross-connect between the OC-N card and the DS-N card.
- Step 7** If the alarm does not clear, clean the far-end optical fiber. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 8** Complete the [Physically Replace a Card, page 2-134](#) for the reporting traffic card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

**Step 9**

If the alarm 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).

## 2.6.137 PLM-V

- Minor (MN), Service Affecting

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

**Note**

In non-revertive UPSR configurations, VT-layer alarms or conditions (ending in \*-V) are not reported when a switch occurs due to VT-level errors. Only **WKSWPR** is reported.

### 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** If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.
- Step 3** If the alarm does not clear, log 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).
- 

## 2.6.138 PRC-DUPID

- Major (MJ), 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** Log into a node on the ring.

- Step 2** Find the node ID by completing the [Identify a Ring ID or Node ID Number, page 2-129](#).
- Step 3** Repeat [Step 2](#) for all the nodes on the ring.
- Step 4** If two nodes have an identical node ID number, complete the [Change a Node ID Number, page 2-129](#) so that each node ID is unique.
- Step 5** If the alarm 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).
- 

## 2.6.139 PROTNA

- Minor (MN), Non-Service Affecting

The Protection Unit Not Available alarm is raised by an out-of-service protection card when a TCC+ or cross-connect card or port that is provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but will clear as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

### Procedure: Clear the PROTNA Alarm

- 
- Step 1** If the PROTNA alarm raises and does not clear, and if it is raised against a common control (TCC+ or cross-connect) card, ensure that there is a redundant control card installed and provisioned in the chassis.
- Step 2** If the alarm is raised against a line card, check whether the facility has been taken out of service.
- a. In CTC, double-click the reporting card to display the card view (if the card is not a cross-connect card).
  - b. Click the **Provisioning** tab.
  - c. Click the **State** of any in-service ports.
  - d. Choose **IS** to take the ports out of service.
- Step 3** Complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.
- While the card resets, the FAIL LED on the physical card will blink and turn off.
  - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 4** Verify that the reset is complete and error-free.
- No new alarms appear in the Alarms tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- Step 5** If the alarm does not clear, complete the [Remove and Reinsert \(Reseat\) a Card, page 2-134](#) for the reporting card.
- Step 6** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
-

## 2.6.140 PWR-A

- Major (MJ), Service Affecting

The NE Power Failure At Connector A alarm applies to the network element (NE) rack. It is raised when there is no power supplied to the main power connector. PWR-A can be raised if power is connected to the backup power connector (Connector B) but not to Connector A, since power must be applied to both supplies.



**Warning**

**Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects will heat up and can cause serious burns or weld the metal object to the terminals.**

### Procedure: Clear the PWR-A Alarm

- 
- Step 1** Verify whether a power connection between the power source and power connector A is present.
  - Step 2** Verify and reseal, if necessary, the connections between the source and the power connector A.
  - Step 3** If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the procedures in NTP-14, “Verify the Shelf Installation,” in the *Cisco ONS 15454 Procedure Guide*.
  - Step 4** If the alarm does not clear, verify the source power output with a voltmeter following the procedures in NTP-14, “Verify the Shelf Installation,” in the *Cisco ONS 15454 Procedure Guide*.
  - Step 5** If the alarm 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).
- 

## 2.6.141 PWR-B

- Major (MJ), Service Affecting

The NE Power Failure at Connector B alarm applies to the NE rack. It is raised when there is no power supplied to the backup power connector. PWR-B can be raised if power is connected to the main power connector (Connector A) but not to Connector B, since power must be applied to both supplies.



**Warning**

**Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects will heat up and can cause serious burns or weld the metal object to the terminals.**

### Procedure: Clear the PWR-B Alarm

- 
- Step 1** Check whether a power connection is present between the power source and power connector B.
  - Step 2** Check and reseal, if necessary, the connections between the source and power connector B.
  - Step 3** If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the procedures in NTP-14, “Verify the Shelf Installation,” in the *Cisco ONS 15454 Procedure Guide*.

- Step 4** If the alarm does not clear, verify the source power output with a voltmeter following the procedures in NTP-14, “Verify the Shelf Installation,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 5** If the alarm 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).
- 

## 2.6.142 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.

To clear the condition, complete the “AIS” [procedure on page 2-16](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.143 RCVR-MISS

- Major (MJ), 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. Incorrect impedance usually occurs when a receive cable is missing from 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** If the attachment is ok, verify that the cabling is securely connected.
- Step 3** If the cabling is ok, verify that the pinouts are correct.
- Step 4** If the pinouts are correct, replace the receive cable.
- Step 5** If the alarm does not clear, log 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).
-

## 2.6.144 RFI-L

- Not Reported (NR) (Condition)

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

RFI-L indicates that the condition 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 node at the far-end node of the reporting ONS 15454.
- Step 2** Check for alarms, especially LOS.
- Step 3** View and clear alarms, especially LOS, by referring to the LOS sections as appropriate.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.145 RFI-P

- Not Reported (NR) (Condition)

A Remote Failure Indication–Path condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-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. The path layer 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.

### Procedure: Clear the RFI-P Condition

- 
- Step 1** Verify that the ports are enabled and in service on the reporting ONS 15454.
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the State column lists the port as IS.



- e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 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** View and clear alarms in the node with the failure, especially **UNEQ-P** or **UNEQ-V**.
- Step 4** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.146 RFI-V

- Not Reported (NR) (Condition)

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



### Note

In non-revertive UPSR configurations, VT-layer alarms or conditions (ending in \*-V) are not reported when a switch occurs due to VT-level errors. Only **WKSWPR** is reported.

## Procedure: Clear the RFI-V Condition

- Step 1** Check connectors to ensure they are securely fastened and connected to the correct slot/port. For more information, refer to NTP-19, “Install the Fiber-Optic Cables,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** If connectors are correctly connected, verify that the DS1-14 port is active and in service.
- a. Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
  - c. Click the **Provisioning > Line** tabs.
  - d. Verify that the State column lists the port as IS.
  - e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 3** If the ports are active and in service, check the signal source for errors using an optical test set.
- Step 4** If the signal is valid, log into the node at the far-end of the reporting ONS 15454.

- Step 5** View and clear alarms in the far-end node, especially [UNEQ-P](#) or [UNEQ-V](#).
- Step 6** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.147 RING-MISMATCH

- Major (MJ), 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** From the node (default view), click the **Provisioning > BLSR** tabs.
- Step 2** Note the number in the *Ring ID* field.
- Step 3** Log into the next ONS node in the BLSR.
- Step 4** Complete the [Identify a Ring ID or Node ID Number, page 2-129](#).
- Step 5** If the ring ID matches the ring ID in the reporting ONS node, repeat [Step 4](#) for the next ONS node in the BLSR.
- Step 6** If the ring ID does not match the ring ID in the reporting ONS node, complete the [Change a Ring ID Number, page 2-129](#).
- Step 7** Verify that the ring map is correct.
- Step 8** Repeat [Step 6](#) for all ONS nodes in the BLSR.
- Step 9** If the alarm 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).
- 

## 2.6.148 RING-SW-EAST

- Not Alarmed (NA) (Condition)

The Ring Switch Is Active–East Side condition occurs when a manual ring switch occurs at the east side of a two-fiber BLSR. The condition clears when the switch is cleared.



#### Note

RING-SW-EAST is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.149 RING-SW-WEST

- Not Alarmed (NA) (Condition)

The Ring Switch Is Active–West Side condition occurs when a manual ring switch occurs at the west side of a two-fiber BLSR. The condition clears when the switch is cleared.

**Note**

RING-SW-WEST is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.150 SD-L

- Not Alarmed (NA) (Condition)

A Signal Degrade–Line condition occurs when the quality of the signal is so poor that the bit error rate on the incoming optical line passed the signal degrade threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and signal fail (SF) both monitor the incoming BER and are similar 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 condition clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** Complete the [Verify BER Threshold Level, page 2-133](#).
- Step 2** If BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.  
For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If the optical power level is ok, verify that optical receive levels are within the acceptable range.
- Step 4** If receive levels are ok, clean the fibers at both ends for a line signal degrade. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.

- Step 5** If the alarm does not clear, verify that single-mode fiber is used.
- Step 6** If the fiber is the correct type, verify that a single-mode laser is used at the far end.
- Step 7** If the problem does not clear, the transmitter at the other end of the optical line may be failing and require replacement.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

- Step 8** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.151 SD-P

- Not Alarmed (NA) (Condition)

A Signal Degrade–Path condition 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 threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

For UPSR protected circuits, the BER threshold on the ONS 15454 is user provisionable and has a range for SD from  $10^{-9}$  to  $10^{-5}$ . For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to  $10^{-6}$ .

On UPSR, an SD-P condition causes a switch from the active card to the standby card at the path (STS) level. On BLSR 1+1 or on unprotected circuits, an SD-P condition does not cause switching.

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**

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

---

**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

---

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** Complete the [Verify BER Threshold Level, page 2-133](#).
- Step 2** If the BER is ok and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If the optical power level is ok, verify that optical receive levels are within the acceptable range.
- Step 4** If the receive level is ok, verify that single-mode fiber is being used.
- Step 5** If the fiber is correct, verify that a single-mode laser is being used at the far end.
- Step 6** If the problem does not clear, the transmitter at the other end of the optical line may be failing and require replacement.

**Caution**

---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

- Step 7** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.152 SF-L

- Not Alarmed (NA) (Condition)

A Signal Fail–Line condition occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure 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**

---

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

---

**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** Complete the [Verify BER Threshold Level, page 2-133](#).
- Step 2** If the BER is ok, and at the expected level, use an optical test set to measure the power level of the line and ensure it is within the guidelines.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If the optical power is ok, verify that optical receive levels are within the acceptable range.
- Step 4** If the receive levels are ok, clean the fibers at both ends for a line signal failure. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 5** If the alarm does not clear, verify that single-mode fiber is being used.
- Step 6** If the correct fiber is used, verify that a single-mode laser is being used at the far-end node.
- Step 7** If the problem does not clear, the transmitter at the other end of the optical line may be failing and need replacement.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

- Step 8** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.153 SF-P

- Not Alarmed (NA) (Condition)

A Signal Fail–Path condition occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure 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.

For UPSR circuits, the BER threshold on the ONS 15454 is user provisionable and has a range for SF from  $10^{-5}$  to  $10^{-3}$ . For BLSR 1+1 or unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to  $10^{-3}$ .

For UPSR, SF-P causes a switch from the active card to the standby card at the path (STS) level. For BLSR 1+1 or unprotected circuits, SF-P does not cause switching.

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**

---

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

---

**Warning**

---

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

---

**Caution**

---

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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** Complete the [Verify BER Threshold Level, page 2-133](#).
- Step 2** If the BER is correct and at the expected level, use an optical test set to measure the power level of the line and ensure it is within the guidelines.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 3** If the optical power level is ok, verify that optical receive levels are within the acceptable range.
- Step 4** If the receive levels are ok, verify that single-mode fiber is being used.
- Step 5** If the fiber is correct, verify that a single-mode laser is being used at the far-end node.
- Step 6** If the problem does not clear, the transmitter at the other end of the optical line may be failing and need replacement.

**Caution**

---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

- Step 7** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
-

## 2.6.154 SFTWDOWN

- Minor (MN), Non-Service Affecting



### Caution

It can take up to 30 minutes for software to be updated on a standby TCC+ card.

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. If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).



### Note

SFTWDOWN is an informational alarm.

## 2.6.155 SNTP-HOST

- Minor (MN), Non-Service Affecting

The SNTP (Simple Network Timing Protocol) Host Failure alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. The forwarding failure can result from two causes, either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

### Procedure: Clear the SNTP-HOST Alarm

- 
- Step 1** Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.
- Step 2** If the ping fails, contact the network administrator who manages the IP network supplying the SNTP information to the proxy and determine whether the network is experiencing problems which may affect the SNTP server/router connecting to the proxy ONS 15454.
- Step 3** If no network problems exist, ensure that the ONS 15454 proxy is provisioned correctly.
- On the ONS node serving as the proxy, click the CTC **Provisioning > General** tabs.
  - Ensure the Enable Proxy checkbox is checked.
  - If the Enable Proxy checkbox is not checked, click it.
- Step 4** If proxy is correctly provisioned, refer to the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.
- Step 5** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.156 SPAN-SW-EAST

- Not Alarmed (NA) (Condition)



The Span Switch Is Active–East Side condition occurs when a force switch occurs at the east side of a four-fiber BLSR span. The condition clears when the switch is cleared.

**Note**

SPAN-SW-EAST is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.157 SPAN-SW-WEST

- Not Alarmed (NA) (Condition)

The Span Switch Is Active–West Side condition occurs when a force switch occurs at the west side of a four-fiber BLSR span. The condition clears when the switch is cleared.

**Note**

SPAN-SW-EAST is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.158 SQUELCH

- Not Alarmed (NA) (Condition)

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance force ring commands. The isolation or failure of the node 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**

**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.
- 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** If fiber continuity is ok, verify that the proper ports are in service.

- a. Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
- b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
- c. Click the **Provisioning > Line** tabs.
- d. Verify that the State column lists the port as IS.
- e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 4** If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.  
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 5** If the signal is valid, verify that the power level of the optical signal is within the optical card's receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.

**Step 6** If the receiver levels are ok, ensure that the optical transmits and receives are connected properly.

**Step 7** If the connectors are ok, complete the [Physically Replace a Card, page 2-134](#) for the OC-N card.



**Caution**

---

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

**Step 8** the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

---

## 2.6.159 SSM-DUS

- Not Alarmed (NA) (Condition)

The Synchronization Status (SSM) Message Quality level Changed to Do-Not-Use (DUS) occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.



**Note**

---

SSM-DUS is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.160 SSM-FAIL

- Minor (MN), Non-Service Affecting

The Failed to Receive Synchronization Status Message alarm occurs when the synchronization status messaging received by the ONS 15454 fails. 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** Verify that SSM is enabled on the external timing source.
- Step 2** If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.
- If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.161 SSM-OFF

- Not Alarmed (NA) (Condition)

The Synchronization Status Messages Disabled on Interface condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS 15454 is set up to receive SSM, but the timing source is not delivering SSM messages.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH line layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

To clear the condition, complete the [“SSM-FAIL” procedure on page 2-113](#). If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.162 SSM-PRS

- Not Alarmed (NA) (Condition)

The SSM Stratum 1 Primary Reference Source Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

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.

**Note**

SSM-PRS is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.163 SSM-RES

- Not Alarmed (NA) (Condition)

The SSM Reserved For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

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.


**Note**


---

SSM-RES is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.164 SSM-SMC

- Not Alarmed (NA) (Condition)

The SSM SONET Minimum Clock Traceable condition occurs when the synchronization message quality level changes to SMC. The NE will not use the clock since it will not use any reference beneath its internal level, which is ST3.

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.


**Note**


---

SSM-SMC is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.165 SSM-ST2

- Not Alarmed (NA) (Condition)

The SSM Stratum 2 Traceable condition occurs when the synchronization message quality level is changed to ST2.

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.


**Note**


---

SSM-ST2 is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.166 SSM-ST3

- Not Alarmed (NA) (Condition)

The SSM Stratum 3 Traceable condition occurs when the synchronization message quality level is changed to ST3.

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.

**Note**

---

SSM-ST3 is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.167 SSM-ST3E

- Not Alarmed (NA) (Condition)

The SSM Stratum 3E Traceable condition indicates the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM, and is not used for Generation 1.

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.

**Note**

---

SSM-ST3E is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.168 SSM-ST4

- Not Alarmed (NA) (Condition)

The SSM Stratum 4 Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used since it is below ST3.

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.

**Note**

---

SSM-ST4 is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.169 SSM-STU

- Not Alarmed (NA) (Condition)

The SSM Synchronization Traceability Unknown condition 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**.
  - Step 5** If the condition 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).
- 

## 2.6.170 SSM-TNC

- Not Alarmed (NA) (Condition)

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

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.



### Note

SSM-TNC is a condition and not an alarm. It is for information only and does not require troubleshooting.

---

## 2.6.171 SWMTXMOD

- Critical, Service Affecting

The Switching Matrix Module Failure alarm occurs on the cross-connect 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 a cross-connect (XCVT) card, it means that a logic component internal to the reporting cross-connect (XCVT) card is out of frame with a second logic component on the same cross-connect card (XCVT). One or more traffic cards may lose traffic as a result of the cross-connect frame failure.

## Procedure: Clear the SWMTXMOD Alarm

- 
- Step 1** If the card reporting the alarm is the standby cross-connect card (XCVT), complete the [Reset a Traffic Card in CTC, page 2-133](#) for the card.
    - While the card resets, the FAIL LED on the physical card will blink and turn off.
    - While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
  - Step 2** Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 3** If the alarm does not clear, complete the [Remove and Reinsert \(Reseat\) a Card, page 2-134](#) for the standby cross-connect card (XCVT).

**Step 4** If the card reporting the alarm is the active cross-connect card (XCVT), complete the [Side Switch the Active or Standby Cross-Connect Card, page 2-131](#).



---

**Note** After the active cross-connect goes into standby, the original standby slot becomes active. The former standby card ACT/STBY LED becomes green.

---

**Step 5** If the card reporting the alarm is not the active cross-connect card (XCVT) or if you completed the side switch in [Step 4](#), complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

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

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 7** If the alarm does not clear, complete the [Remove and Reinsert \(Reseat\) a Card, page 2-134](#) for the standby cross-connect (XCVT) card.

**Step 8** If the card reporting the alarm is an I/O card, complete the [Side Switch the Active or Standby Cross-Connect Card, page 2-131](#).

**Step 9** If the alarm does not clear after the cross-connect card (XC, XCVT, XC10G) side switch, complete the [Reset a Traffic Card in CTC, page 2-133](#) for the reporting card.

- While the card resets, the FAIL LED on the physical card will blink and turn off.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.

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

- No new alarms appear in the Alarms tab on CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

**Step 11** If the alarm does not clear, complete the [Remove and Reinsert \(Reseat\) a Card, page 2-134](#) for the traffic line card.

**Step 12** If the alarm 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).

---

## 2.6.172 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**

SWTOPRI is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.173 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.

To clear the condition, view and clear alarms related to failures of the primary source, such as the [SYNCPRI](#) alarm. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.174 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.

To clear the condition, view and clear alarms related to failures of the primary source, such as the [SYNCPRI](#) and [SYNSEC](#) alarms. If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.175 SYNC-FREQ

- Not Alarmed (NA) (Condition)

The Synchronization Reference Frequency Out Of Bounds condition is reported against any reference that is out of the bounds for valid references. The NE will fail the reference and choose another internal or external reference to use.

### Procedure: Clear the SYNC-FREQ Condition

- 
- Step 1** Use an optical test set to check the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency:



For BITS, the proper timing frequency range is approximately -15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately -16 PPM to 16 PPM.

- Step 2** If the reference source frequency is not outside of bounds, complete the [Physically Replace a Card](#), page 2-134 for 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.



**Note** It takes up to 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 the transfer 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 3** If the SYNC-FREQ alarm continues to report after replacing the TCC+ card, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.176 SYNCPRI

- Minor (MN), 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). Switching to the secondary timing source also triggers the [SWTOSEC](#) alarm.

### Procedure: Clear the SYNCPRI Alarm

- Step 1** From the CTC node (default login) view, click the **Provisioning > Timing** tabs.
- Step 2** Check the current configuration for the REF-1 of the NE Reference.
- Step 3** If the primary reference is a BITS input, complete the [“LOS \(BITS\)” procedure on page 2-79](#).
- Step 4** If the primary reference clock is an incoming port on the ONS 15454, complete the [“LOS \(OC-N\)” procedure on page 2-82](#).
- Step 5** If the condition does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

## 2.6.177 SYNCSEC

- Minor (MN), 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. Switching to the third timing source also triggers the [SWTOTHIRD](#) condition.

## Procedure: Clear the SYNCSEC Alarm

- 
- Step 1** From the CTC node (default login) view, click the **Provisioning > Timing** tabs.
  - Step 2** Check the current configuration of the REF-2 for the NE Reference.
  - Step 3** If the secondary reference is a BITS input, complete the [“LOS \(BITS\)” procedure on page 2-79](#).
  - Step 4** Check that the BITS clock is operating properly.
  - Step 5** If the secondary timing source is an incoming port on the ONS 15454, complete the [“LOS \(OC-N\)” procedure on page 2-82](#).
  - Step 6** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 2.6.178 SYNCTHIRD

- Minor (MN), 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, the TCC+ card may have failed. The ONS 15454 often reports either [FRNGSYNC](#) or [HLDVRSYNC](#) 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 CTC node (default login) view, click the **Provisioning > Timing** tabs.
  - Step 2** Check the current configuration of the REF-3 for the NE Reference. For more information about references, refer to NTP-28, “Set Up Timing,” in the *Cisco ONS 15454 Procedure Guide*.
  - Step 3** If the third timing source is a BITS input, complete the [“LOS \(BITS\)” procedure on page 2-79](#).
  - Step 4** If the third timing source is an incoming port on the ONS 15454, complete the [“LOS \(OC-N\)” procedure on page 2-82](#).
  - Step 5** If the third timing source uses the internal ONS 15454 timing, complete the [Reset the Active TCC+ Card in CTC, page 2-133](#).

Wait ten minutes to verify that the card you reset completely reboots and displays as Standby. If not, call the Cisco Technical Assistance Center (1-800-553-2447).

- Step 6** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+”](#) section on page 3-4.
- Step 7** If the alarm has not cleared, call the Cisco Technical Assistance Center (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC+”](#) procedure on page 3-4. If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card”](#) procedure on page 2-134.
- 

## 2.6.179 SYSBOOT

- Major (MJ), Service Affecting

The System Reboot alarm indicates that new software is booting on the TCC+ card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If it 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).

**Note**

SYSBOOT is an informational alarm and does not require troubleshooting.

---

## 2.6.180 TIM-P

- Minor (MN), Service Affecting

The STS Path Trace Identifier Mismatch (TIM) Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the New Expected String field for the receiving port. The 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, the circuit path has changed or someone entered a new incorrect value into the New Transmit String field. Follow the procedure below to clear either instance.

TIM-P 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. TIM-P is usually accompanied by other alarms, such as LOS, UNEQ-P, or PLM-P. If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

### 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 choose **Edit Path Trace** from the shortcut menu.

- Step 5** On the detailed circuit map, right-click the drop/destination circuit port and choose **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**.
  - Step 9** If the alarm 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).
- 

## 2.6.181 TPTFAIL

- Major (MJ), Service Affecting

The Transport (TPT) Layer Failure alarm indicates a break in the end-to-end Ethernet link integrity feature of the G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port, which prevents the complete end-to-end Ethernet path from working. If any SONET path alarm such as AIS-P, LOP-P, UNEQ-P, or PDI-P exists 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 the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter and also cause a CARLOSS condition to occur on the reporting port. In all cases the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

### 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 the port is using or with the far end G1000-4 port that is mapped to the port. View and clear 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 if 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. View and clear any alarms, such as CARLOSS, reported against the far-end port or card.
  - Step 3** If the alarm 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).
- 

## 2.6.182 TRMT

- Major (MJ), Service Affecting

A Missing Transmitter 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** Complete the [Physically Replace a Card, page 2-134](#) for the reporting DS1-14 card.



**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.



**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** If the alarm does not clear, call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).

---

## 2.6.183 TRMT-MISS

- Major (MJ), 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. Incorrect impedance is detected when a 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** If the device is operational, verify that the cabling is securely connected.

**Step 3** If the cabling is secure, verify that the pinouts are correct.

**Step 4** If the pinouts are correct, replace the transmit cable.

**Step 5** If the alarm does not clear, log 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).

---

## 2.6.184 UNEQ-P

- Critical, Service Affecting

A 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.

The alarm may result from an incomplete circuit or an empty VT tunnel, which is a VT tunnel with no valid VT circuit inside. Empty VT tunnels can result when a user highlights both a VT tunnel and VT circuit in CTC and attempts to delete them simultaneously. If the user attempts double deletion, CTC will delete only the VT circuit. The empty VT tunnel raises an UNEQ-P alarm.

UNEQ-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. The path 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.



### 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.
- Step 2** Right-click the alarm to display the Select Affected Circuits dialog.
- Step 3** Click the Select Affected Circuits dialog.
- Step 4** When the Affected Circuits appear, look in the Type column for VTT, which indicates a VT tunnel Circuit. A VT tunnel with no VTs assigned may be the cause of an UNEQ-P alarm.
- Step 5** If the Type column does not contain VTT there are no VT tunnels connected with the alarm, go to [Step 7](#).
- Step 6** If the Type column does contain VTT, attempt to delete these row(s).



### Note

The CTC will not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

- a. Click the VT tunnel circuit row to highlight it. Complete the [Delete a Circuit, page 2-132](#).
- b. If an error message dialog appears, the VT tunnel is valid and not the cause of the alarm.
- c. If any other columns contain VTT, repeat [Step 6](#).

- Step 7** If all ONS nodes in the ring appear in the CTC network view, check for incomplete circuits.
- Click the **Circuits** tab.
  - Verify that INCOMPLETE is not listed in the State column of any circuits.
- Step 8** If you find circuits listed as incomplete, verify these circuits are not working circuits that continue to pass traffic with an appropriate optical test set and site-specific procedures.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 9** If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.
- Click the row under the State column with incomplete and complete the [Delete a Circuit, page 2-132](#).
- Step 10** Log back in and verify that all circuits terminating in the reporting card are active.
- Click the **Circuits** tab.
  - Verify that the State column lists all circuits as active.
- Step 11** If the alarm does not clear, clean the far-end optical fiber. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.

**Warning**

**On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**

**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

- Step 12** If the alarm does not clear, log 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).

## 2.6.185 UNEQ-V

- Major (MJ), Service Affecting

An Signal Label Mismatch Failure Unequipped–VT alarm indicates that the node is receiving SONET path overhead with bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is 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 card (XC/XCVT/XC10G) and the corresponding DS-N card.

**Warning**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).

**Warning**

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.

**Caution**

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

**Note**

In non-revertive UPSR configurations, VT-layer alarms or conditions (ending in \*-V) are not reported when a switch occurs due to VT-level errors. Only **WKSWPR** is reported.

## Procedure: Clear the UNEQ-V Alarm

- Step 1** Verify that all circuits terminating in the reporting card are active.
- Click the **Circuits** tab.
  - Verify that the State column lists the port as active.
  - 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, complete the [Delete a Circuit, page 2-132](#).



**Caution** Deleting a circuit can be service affecting.

- Step 4** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures about how to create circuits.
- Step 5** If circuit deletion and recreation does not clear the alarm, check the far-end OC-N card that provides STS payload to the DS-N card.
- Step 6** If the far-end card is ok, verify the cross-connect between the OC-N card and the DS-N card.
- Step 7** If the cross-connect is ok, clean the far-end optical fiber. Complete NTP-112, “Clean Fiber Connectors,” in the *Cisco ONS 15454 Procedure Guide*.
- Step 8** If the alarm does not clear, complete the [“Physically Replace a Card” section on page 2-134](#) for the OC-N/DS-N cards.



**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

**Note**

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

**Step 9**

If the alarm 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).

## 2.6.186 WKS WPR

- Not Alarmed (NA) (Condition)

The Working Switched To Protection condition is raised when a line experiences an LOS, signal fail, or signal degrade. Troubleshoot using the LOS procedure.

**Note**

WKS WPR is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.6.187 WTR

- Not Alarmed (NA) (Condition)

The Wait To Restore condition indicates that revertive switching is specified and that a WKS WPR occurred, and although the working path is good again, the wait to restore timer has not expired. The alarm clears when the timer expires and traffic is switched back to the working path.

**Note**

WTR is a condition and not an alarm. It is for information only and does not require troubleshooting.

## 2.7 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 2-8 DS3-12E Line Alarms**

| <b>Alarm</b>                | <b>UNFRAMED</b> | <b>M23</b> | <b>CBIT</b> |
|-----------------------------|-----------------|------------|-------------|
| 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    | ○               | ○          | ◆           |

## 2.8 Common Procedures in Alarm Troubleshooting

This section gives common procedures that are frequently used when troubleshooting alarms. For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure: Identify a Ring ID or Node ID Number

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** From the View menu, choose Go to Network View.
  - Step 3** Click the **Provisioning > BLSR** tabs.  
From the Ring ID column, record the ring ID, or from the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.
- 

### Procedure: Change a Ring ID Number

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** From the View menu, choose Go to Network View.
  - Step 3** Click the **Provisioning > BLSR** tabs.
  - Step 4** Highlight the row of the ring and click **Edit**.
  - Step 5** In the BLSR window, enter the new ID in the *Ring ID* field.
  - Step 6** Click **Apply**.
  - Step 7** Click **Yes** at the Changing Ring ID dialog box.
- 

### Procedure: Change a Node ID Number

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** From the View menu, choose Go to Network View.
  - Step 3** Click the **Provisioning > BLSR** tabs.
  - Step 4** Highlight the ring and click **Edit**.
  - Step 5** In the BLSR window, right-click the node on the ring map.
  - Step 6** Select Set Node ID from the shortcut menu.
  - Step 7** Enter the new ID in the field.
  - Step 8** Click **Apply**.
-

## Procedure: Verify Node Visibility for Other Nodes

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** At the node (default) view, click the **Provisioning > BLSR** tabs.
  - Step 3** Highlight a BLSR.
  - Step 4** Click **Ring Map**.
  - Step 5** Verify that each node in the ring appears on the ring map with a node ID and IP address.
  - Step 6** Click **Close**.
- 

## Procedure: Check or Create Node SDCC Terminations

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** At the node (default) view, click the **Provisioning > SONET DCC** tabs.
  - Step 3** View the Port column entries to see where terminations are present for a node. If all terminations are not present, proceed to [Step 4](#).
  - Step 4** If necessary, create an SDCC termination.
    - a. Click **Create**.
    - b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.
    - c. In the Port State area, click the Set to IS, if allowed radio button.
    - d. Verify the Disable OSPF on DCC Link checkbox is unchecked.
    - e. Click **OK**.
- 

## Procedure: Lock Out a BLSR Span

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** In the node (default CTC login view), click the **Maintenance > BLSR** tabs.
  - Step 3** Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.
  - Step 4** Choose **LOCKOUT SPAN** and click **Apply**.
  - Step 5** Click **OK** on the BLSR Operations dialog box.
- 

## Procedure: Clear a BLSR Span Command

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
- Step 2** In the node (default CTC login view), click the **Maintenance > BLSR** tabs.

- Step 3** Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.
  - Step 4** Choose **CLEAR** and click **Apply**.
  - Step 5** Click **OK** on the BLSR Operations dialog box.
- 

## Procedure: Clear a UPSR Lockout

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** From the View menu, choose Go to Network View.
  - Step 3** Right-click the span where you want to clear the switch. Choose Circuits from the shortcut menu.
  - Step 4** On the Circuits on Span dialog box, choose CLEAR to remove a previously set switch command. Click **Apply**.
  - Step 5** On the Confirm UPSR Switch dialog box, click **Yes**.
  - Step 6** On the Protection Switch Result dialog box, click **OK**.  
On the Circuits on Span window, the Switch State for all UPSR circuits is CLEAR.
- 

## Procedure: Move Protection Group Traffic with a Switch Command

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** Display the CTC node (default login) view.
  - Step 3** At the CTC node (default login) view, click the **Maintenance > Protection** tabs.
  - Step 4** Double-click the protection group that contains the reporting card.
  - Step 5** Click the Working/Active card of the selected groups.
  - Step 6** Click **Switch** and **Yes** in the Confirmation dialog box.
- 

## Procedure: Side Switch the Active or Standby Cross-Connect Card

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
- Step 2** Display the CTC node (default login) view.
- Step 3** Determine the active or standby cross-connect card.  
The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.



**Note** You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

---

- Step 4** In the CTC node (default login) view, select the **Maintenance > XC Cards** tabs.
- Step 5** Click **Switch**.

**Step 6** Click **Yes** in the Confirm Switch dialog box.

---

## Procedure: Clear a Protection Group Switch Command

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** Display the CTC node (default login) view.
  - Step 3** At the CTC node (default login) view, click the **Maintenance > Protection** tabs.
  - Step 4** Double-click the protection group that contains the reporting card.
  - Step 5** Highlight either selected group.
  - Step 6** Click **Clear** and click **Yes** at the confirmation dialog box.
- 

## Procedure: Delete a Circuit

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** Display the CTC node (default login) view.
  - Step 3** Click the **Circuits** tab.
  - Step 4** Click the circuit row to highlight it and click **Delete**.
  - Step 5** Click **Yes** at the Delete Circuits dialog box.
- 

## Procedure: Clear a Loopback

---

- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** Double-click the reporting card in CTC to display the card view.
  - Step 3** Click the **Maintenance** tab.
  - Step 4** In the Loopback Type column, see whether any port row displays a state besides None.
  - Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
  - Step 6** In the State column, see whether any port row displays a state besides INS.
  - Step 7** If a row contains another state besides INS, click in the column cell to display the drop-down list and select INS.
  - Step 8** Click **Apply**.
-

## Procedure: Reset the Active TCC+ Card in CTC

- 
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
- Step 2** Identify the active TCC+.
- If you are looking at the physical ONS 15454, the ACT/STBY LED of active TCC+ is green.
  - If you are looking at the CTC node (default login) view of the ONS 15454, the standby TCC+ has a green LED depiction with the letters “Act.”
- Step 3** Right-click the active TCC+.
- Step 4** Choose **Reset Card** from the shortcut menu.
- Step 5** Click **Yes** at the Are You Sure dialog box.
- The card resets, the FAIL LED blinks on the physical card, and then no LED will be illuminated.
- While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- Step 6** Verify that the reset is complete and error-free.
- No new alarms appear in the **Alarms** tab on CTC.
  - If you are looking at the physical ONS 15454, the ACT/STBY LED is steadily illuminated amber.
  - If you are looking at the CTC node (default login) view of the ONS 15454, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- 

## Procedure: Reset a Traffic Card in CTC

- 
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
- Step 2** Display the CTC node (default login) view.
- Step 3** Position the cursor over the slot reporting the alarm.
- Step 4** Right-click and choose **RESET CARD** from the shortcut menu.
- 

## Procedure: Verify BER Threshold Level

- 
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
- Step 2** Display the CTC node (default login) view.
- Step 3** From the CTC node (default login) view, double-click the card reporting the alarm to display the card view.
- Step 4** Click the **Provisioning > Line** tabs.
- Step 5** Under the SD BER column on the Provisioning pane, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.
- Step 6** If the entry is consistent with what the system was originally provisioned for, continue to [Step 2](#).

- Step 7** 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.
- Step 8** Click **Apply**.
- 

## Procedure: Physically Replace a Card



### Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Consult the *Cisco ONS 15454 Procedure Guide* for information.

---

- Step 1** Open the card ejectors.
- Step 2** Slide the card out of the slot.
- Step 3** Open the ejectors on the replacement card.
- Step 4** Slide the replacement card into the slot along the guide rails.
- Step 5** Close the ejectors.
- 

## Procedure: Remove and Reinsert (Reseat) a Card

- Step 1** Open the card ejectors.
- Step 2** Slide the card halfway out of the slot along the guide rails.
- Step 3** Slide the card all the way back into the slot along the guide rails.
- Step 4** Close the ejectors.
- 

## Procedure: Remove and Reinsert Fan Tray

- Step 1** Use the retractable handles embedded in the front of the fan tray to pull the fan-tray assembly forward several inches.
- Step 2** Push the fan-tray assembly firmly back into the ONS 15454.
- Step 3** Close the retractable handles.
-





## Replace Hardware

---

This chapter provides procedures for replacing Cisco ONS 15454 hardware.

Every section is a procedure.

1. [Switch Traffic and Replace an In-Service Cross-Connect Card, page 3-1](#)—Complete this procedure to replace and in-service cross-connect card.
2. [Remove and Reinsert \(Reseat\) the Standby TCC+, page 3-4](#)—Complete this procedure as needed to reset the TCC+ by performing a card pull.
3. [Replace the Air Filter, page 3-5](#)—Complete this procedure to replace a reusable or disposable air filter.
4. [Determine Replacement Hardware Compatibility, page 3-9](#)—Complete this procedure to verify replacement hardware compatibility.
5. [Replace the Fan-Tray Assembly, page 3-11](#)—Complete this procedure to replace the fan-tray assembly.
6. [Replace the Alarm Interface Panel, page 3-13](#)—Complete this procedure to replace the alarm interface panel (AIP).
7. [Replace the Electrical Interface Assembly, page 3-19](#)—Complete this procedure to replace the electrical interface assembly (EIA).

### 3.1 Switch Traffic and Replace an In-Service Cross-Connect Card

|                                |                                                           |
|--------------------------------|-----------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an in-service cross-connect card. |
| <b>Tools/Equipment</b>         | Replacement cross-connect card                            |
| <b>Prerequisite Procedures</b> | None                                                      |
| <b>Required/As Needed</b>      | As needed                                                 |
| <b>Onsite/Remote</b>           | Onsite                                                    |



**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.**

---

**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/XC10G card 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 cross-connect card (XC/XCVT/XC10G) without a lockout will cause UPSR circuits to switch.

**Step 1**

Log into the node where you will perform the cross-connect card (XC/XCVT/XC10G) replacement:

- a. From your PC, start Netscape or Internet Explorer.
- b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments.

- c. In the Login dialog box, type your name and password. (Both are case sensitive.)
- d. Each time you log into an ONS 15454, you can make selections on the following login options:
  - *Node Name*—Displays the IP address entered in the web browser and a pull-down menu of previously-entered ONS 15454 IP addresses. You can select any ONS 15454 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
  - *Additional Nodes*—Displays a list of login node groups that were created. (To create a login node group or add additional groups, see the *Cisco ONS 15454 Procedure Guide*.)

**Note**

Topology hosts that were created in previous ONS 15454 releases by modifying the ctc.ini file are displayed as a “Topology Host” group under Additional Nodes.

- *Exclude Dynamically Discovered Nodes*—Check this box to view only the ONS 15454 (and login node group members, if any) entered in the *Node Name* field. Nodes linked to the *Node Name* ONS 15454 through the DCC are not displayed. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.

- e. Click **Login**.

**Step 2**

Ensure the working span is active on both local and remote nodes:

- a. In node (default login) view, click the **Maintenance > BLSR** tabs.
- b. Locate the applicable span.

In the West Line and East Line columns, the working/active span is identified by (Work/Act).

**Step 3**

Ensure the working span is carrying error-free traffic (no SD or SF alarms present). Display the network view and click the **Alarms** tab to display alarms.

**Step 4** Lock out the protection span according to the specific protection scheme:

a. Lock out the protection span in a BLSR protection scheme:

- In node (default login) view, click the **Maintenance > BLSR** tabs. Locate the applicable span. In the West Line and East Line columns, the working/active span is identified by (Work/Act). Place a lockout on the East and West cards of the nodes adjacent to the XC switch node. For example, to switch the cross-connect card (XC) on Node B, place a lockout on the West card of Node A and on the East card of Node C, no lockout is necessary on Node B.

<-----East [Node A] West-----East [Node B] West-----East [Node C] West----->

Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost. Choose the correct row for the span and then under the West Switch column, choose **LOCOUT SPAN** from the list box.

b. Lock out the protection span in a 1+1 protection scheme:

- In node (default login) view, click the **Maintenance > Protection** tabs.
- Choose the affected 1+1 protection group from the Protection Groups window.
- In the Selected Group window, the working and protect spans appear. Choose the **protect/standby card** and click **Lock Out**.
- Click **Yes** on the confirmation dialog box.



**Note** A cross-connect card (XC/XCVT/XC10G) reset can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

c. Lock out the protection span in a UPSR protection scheme:

- Click the **Circuits** tab.
- Locate the span row.
- Under the Switch State column, click the **Switch all UPSR- circuits away** menu.
- Choose **Clear** and click **Apply**.
- Click **Yes** at the Confirm UPSR Switch Are You Sure? dialog box.
- Click **OK** at the confirmation dialog box.



**Caution** The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

**Step 5** When the protection span has been locked out, determine the active cross-connect card (XC/XCVT/XC10G). 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 6** Switch the active cross-connect card (XC/XCVT/XC10G) to standby:

- In the node (default login) view, click the **Maintenance > XC Cards** tabs.
- Under Cross Connect Cards, choose **Switch**.

- c. Click **Yes** on the Confirm Switch dialog box.



**Note** After the active XC/XCVT/XC10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

**Step 7** Physically remove the new standby cross-connect card (XC/XCVT/XC10G) from the ONS 15454.

**Step 8** Insert the replacement cross-connect card (XC/XCVT/XC10G) into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

**Step 9** Release the protection lockout(s) applied in [Step 4](#):

- a. Log into the node where you will clear the lockout.
- b. Click the **Maintenance > Protection** tabs.
- c. Under Protection Groups, click the protection group that contains the card you want to clear.
- d. Under Selected Group, click the card you want to clear.
- e. Click **Clear**.
- f. Click **Yes** on the confirmation dialog box.

The lockout is cleared.

## 3.2 Remove and Reinsert (Reseat) the Standby TCC+

|                                |                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------|
| <b>Purpose</b>                 | Use this procedure to reset the TCC+ card by removing and reinserting the card. |
| <b>Tools/Equipment</b>         | None                                                                            |
| <b>Prerequisite Procedures</b> | None                                                                            |
| <b>Required/As Needed</b>      | As needed                                                                       |
| <b>Onsite/Remote</b>           | Onsite                                                                          |



### Caution

Do not perform this action without the supervision and direction of the Cisco Technical Assistance Center (TAC). The Cisco TAC can be reached at (1-800-553-2447).



### 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** Ensure that the TCC+ you want to reset is in standby mode. On the TCC+ card, the ACT/STBY (Active/Standby) LED is amber when the TCC+ is in standby mode.

**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. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about LED behavior during TCC+ reboots.

## 3.3 Replace the Air Filter

|                                |                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | The following procedure describes how to replace reusable and disposable air filters. |
| <b>Tools/Equipment</b>         | Spare air filters                                                                     |
| <b>Prerequisite Procedures</b> | None                                                                                  |
| <b>Required/As Needed</b>      | As needed                                                                             |
| <b>Onsite/Remote</b>           | Onsite                                                                                |

**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.**

**Note**

Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

- Step 1** To replace the reusable air filter, complete the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) task on page 3-5.
- Step 2** To replace the disposable air filter, complete the [“Inspect and Replace the Disposable Air Filter”](#) task on page 3-7.

### 3.3.1 Inspect, Clean, and Replace the Reusable Air Filter

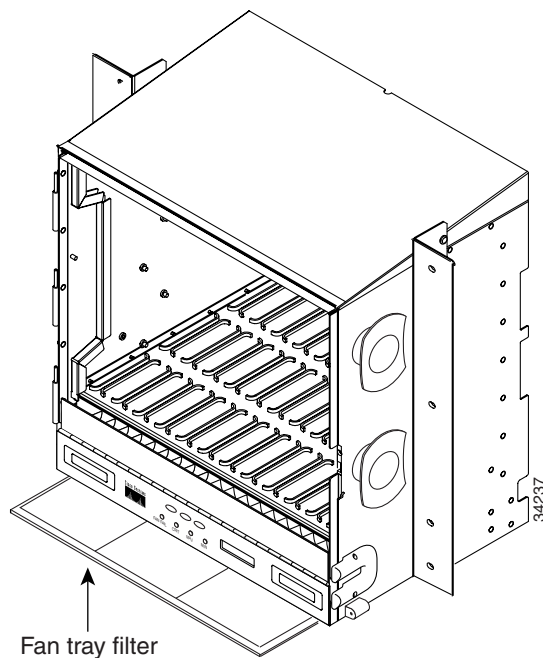
|                                |                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This task ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf. |
| <b>Tools/Equipment</b>         | Vacuum or detergent and water faucet, spare filter, pinned hex key                                                                                  |
| <b>Prerequisite Procedures</b> | None                                                                                                                                                |
| <b>Required/As Needed</b>      | Inspection required every 30 days. Clean as needed.                                                                                                 |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                              |

- Step 1** Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.

- Step 2** If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that may have collected on the filter and proceed to [Step 3](#). [Figure 3-1](#) illustrates a reusable fan-tray air filter in an external filter bracket. If the filter is installed beneath the fan tray and not in the external filter brackets:
- a. Open the front door of the shelf assembly.
    - Open the front door lock.
 

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
    - Press the door button to release the latch.
    - Swing the door open.
  - b. Remove the front door (optional). If you do not want to remove the door, proceed to [Step 3](#):
    - Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
    - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
    - Secure the dangling end of the ground strap to the door or chassis with tape.

**Figure 3-1** A reusable fan-tray air filter in an external filter bracket (front door removed)



- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 5** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 6** Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that may have collected on the filter.
- Step 7** Visually inspect the air filter material for dirt and dust.

**Step 8** If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.



**Note** Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

**Step 9** If you washed the filter, allow it to completely air dry for at least eight hours.



**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, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.



**Caution** If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.



**Note** On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

**Step 10** To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

**Step 11** Rotate the retractable handles back into their compartments.

**Step 12** If you replace the door, also reattach the ground strap.

**Step 13** Close and lock the door.

## 3.3.2 Inspect and Replace the Disposable Air Filter

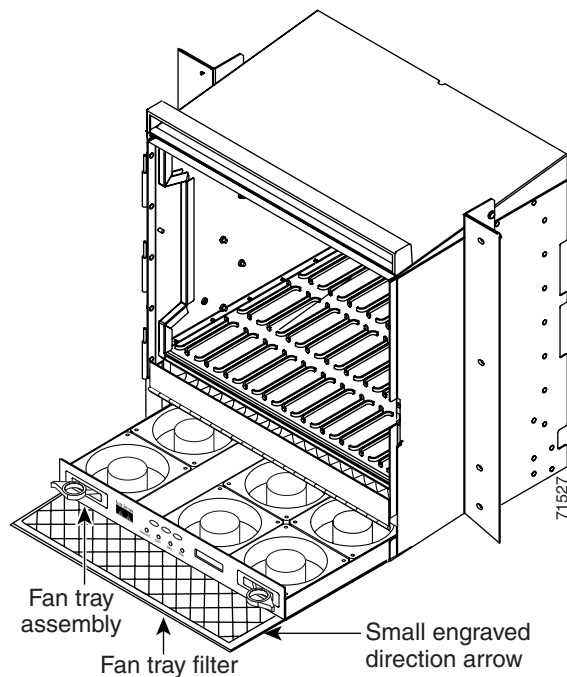
|                                |                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This task ensures that the air filter is free from dirt and dust to allow optimum air flow and prevent dirt and dust from entering the ONS 15454. |
| <b>Tools/Equipment</b>         | Extra filters, pinned hex key                                                                                                                     |
| <b>Prerequisite Procedures</b> | None                                                                                                                                              |
| <b>Required/As Needed</b>      | Inspection required every 30 days. Replace as needed.                                                                                             |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                            |

**Note**

The disposable air filter is installed beneath the fan-tray assembly only, so you must remove the fan-tray assembly to inspect and replace the disposable air filter.

- Step 1** Verify that you are replacing a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. NEBS 3E and earlier versions of the ONS 15454 use a disposable air filter.
- Step 2** Open the front door of the shelf assembly:
- Open the front door lock.  
The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
  - Press the door button to release the latch.
  - Swing the door open.
- Step 3** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 4](#).
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 4** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 5** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly ([Figure 3-2](#)).

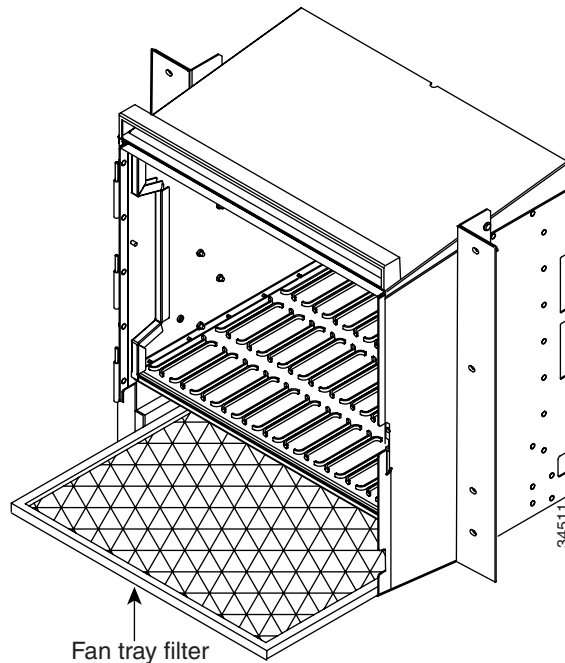
**Figure 3-2** Inserting or removing the fan-tray assembly (front door removed)





- Step 7** Gently remove the air filter from the shelf assembly (Figure 3-3). Be careful not to dislodge any dust that may have collected on the filter.
- Step 8** Visually inspect the white filter material for dirt and dust.
- Step 9** If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter by sliding the 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 (front door removed)



- Step 10** 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 11** To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.
- Step 12** Rotate the retractable handles back into their compartments.
- Step 13** If you replace the door, also reattach the group strap.
- Step 14** Close and lock the door.

## 3.4 Determine Replacement Hardware Compatibility

|                                |                                                               |
|--------------------------------|---------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure determines replacement hardware compatibility. |
| <b>Tools/Equipment</b>         | None                                                          |
| <b>Prerequisite Procedures</b> | None                                                          |

**Required/As Needed** Required when replacing the fan-tray assembly and AIP.  
**Onsite/Remote** Both

**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 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC10G, OC-192, and OC-48AS cards.

**Note**

The 5A AIP (73-7665-XX) is required when installing the 15454-FTA3 fan-tray assembly.

**Step 1**

Review [Table 3-1](#) to ensure you have compatible components when replacing the fan-tray assembly or the AIP and note the alarms that will occur when an incompatible combination of hardware is installed.

**Note**

If you need to determine the hardware that has been installed on a node, click the inventory tab in node (default login) view.

**Table 3-1 Incompatibility Alarms**

| Shelf Assembly <sup>1</sup> | Fan Tray <sup>2</sup> | AIP <sup>3</sup> | 10G Cards <sup>4</sup> | Ethernet Cards <sup>5</sup> | Alarms                         |
|-----------------------------|-----------------------|------------------|------------------------|-----------------------------|--------------------------------|
| —                           | —                     | No fuse          | —                      | —                           | MEA on AIP                     |
| NEBS3E or NEBS3             | 2A                    | 2A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 2A                    | 2A               | Yes                    | —                           | MEA on 10G                     |
| NEBS3E or NEBS3             | 2A                    | 5A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 2A                    | 5A               | Yes                    | —                           | MEA on 10G                     |
| NEBS3E or NEBS3             | 5A                    | 2A               | No                     | —                           | MEA on fan tray                |
| NEBS3E or NEBS3             | 5A                    | 2A               | Yes                    | —                           | MEA on fan tray and 10G cards  |
| NEBS3E or NEBS3             | 5A                    | 5A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 5A                    | 5A               | Yes                    | —                           | MEA on 10G                     |
| ANSI                        | 2A                    | 2A               | No                     | —                           | None                           |
| ANSI                        | 2A                    | 2A               | Yes                    | 2.5G compatible             | MEA on fan tray, AIP, Ethernet |
| ANSI                        | 2A                    | 2A               | Yes                    | 10G compatible              | MEA on fan tray, AIP           |
| ANSI                        | 2A                    | 5A               | No                     | Either                      | None                           |
| ANSI                        | 2A                    | 5A               | Yes                    | 2.5G compatible             | MEA on fan tray, Ethernet      |

**Table 3-1 Incompatibility Alarms (continued)**

| Shelf Assembly <sup>1</sup> | Fan Tray <sup>2</sup> | AIP <sup>3</sup> | 10G Cards <sup>4</sup> | Ethernet Cards <sup>5</sup> | Alarms               |
|-----------------------------|-----------------------|------------------|------------------------|-----------------------------|----------------------|
| ANSI                        | 2A                    | 5A               | Yes                    | 10G compatible              | MEA on fan tray      |
| ANSI                        | 5A                    | 2A               | No                     | Either                      | MEA on AIP           |
| ANSI                        | 5A                    | 2A               | Yes                    | 2.5G compatible             | MEA on AIP, Ethernet |
| ANSI                        | 5A                    | 2A               | Yes                    | 10G compatible              | MEA on AIP           |
| ANSI                        | 5A                    | 5A               | No                     | Either                      | None                 |
| ANSI                        | 5A                    | 5A               | Yes                    | Either                      | None                 |

- 15454-SA-ANSI (P/N: 800-19857-01) = ONS 15454 Release 3.1 and later shelf assembly, 15454-SA-NEBS3E (P/N: 800-07149-xx) or 15454-SA-NEBS3 (P/N: 800-06741-xx) = shelf assemblies released before ONS 15454 Release 3.1
- 5A Fan Tray = 15454-FTA3 (P/N: 800-19858-xx) or 15454-FTA3-T (P/N: 800-21448-xx), 2A Fan Tray = 15454-FTA2 (P/Ns: 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx)
- 5A AIP (P/N: 73-7665-01), 2A AIP (P/N: 73-5262-01)
- 10G cards = XC-10G, OC-192, OC-48AS
- 2.5G compatible Ethernet cards = E1000-T, E1000-2, E1000T-G, E10002-G, G1000-4  
10G compatible Ethernet cards = E1000T-G, E10002-G, G1000-4

**Step 2** See the “[Replace the Fan-Tray Assembly](#)” section on page 3-11 to replace the fan-tray assembly or the “[Inspect and Replace the Disposable Air Filter](#)” section on page 3-7 to replace the AIP.

## 3.5 Replace the Fan-Tray Assembly

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities. You can remove the fan-tray assembly using the retractable handles and replace it by pushing until it plugs into the receptacle on the back panel.

|                                |                                                                        |
|--------------------------------|------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing FTA with a new FTA.                |
| <b>Tools/Equipment</b>         | None                                                                   |
| <b>Prerequisite Procedures</b> | <a href="#">Determine Replacement Hardware Compatibility, page 3-9</a> |
| <b>Required/As Needed</b>      | As needed                                                              |
| <b>Onsite/Remote</b>           | Onsite                                                                 |



**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.



**Caution**

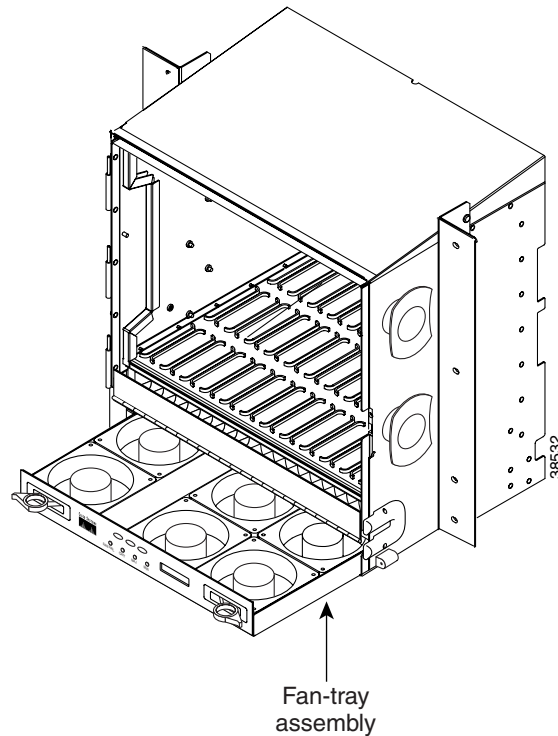
Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.

**Note**

The 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

- 
- Step 1** Open the front door of the shelf assembly:
- Open the front door lock.  
The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
  - Press the door button to release the latch.
  - Swing the door open.
- Step 2** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 3](#).
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Fold out the retractable handles at the outside edges of the fan tray.
- Step 5** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. [Figure 3-4](#) shows the location of the fan tray.
- Step 7** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
- If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [“Replace the Air Filter” section on page 3-5](#).
- Step 8** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 9** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.
- Step 10** If you replace the door, also reattach the ground strap.
- Step 11** Close and lock the door.

**Figure 3-4** Removing or replacing the fan-tray assembly (front door removed)



## 3.6 Replace the Alarm Interface Panel

|                                |                                                                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing AIP with a new AIP on an in-service system without affecting traffic (except Ethernet circuits) |
| <b>Tools/Equipment</b>         | #2 Phillips screwdriver                                                                                                             |
| <b>Prerequisite Procedures</b> | <a href="#">Determine Replacement Hardware Compatibility, page 3-9</a>                                                              |
| <b>Required/As Needed</b>      | As needed                                                                                                                           |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                              |



**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**

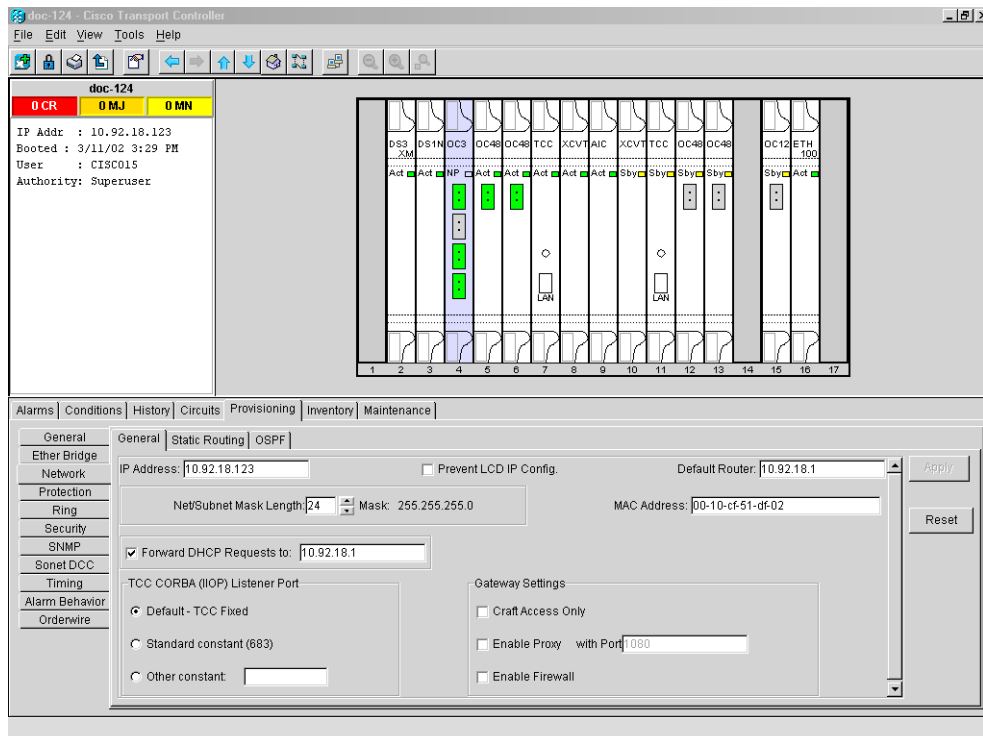
Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

**Note**

Perform this procedure in a maintenance window. Resetting the active TCC+ can cause a service disruption of less than 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:
- Log into CTC. See [Step 1](#) in the “Switch Traffic and Replace an In-Service Cross-Connect Card” procedure on page 3-1 for instructions.
  - In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
  - 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:
- Log into the node where you will replace the AIP. For login procedures, see the *Cisco ONS 15454 Procedure Guide*.
  - In node (default login) view, click the **Provisioning > Network** tabs.
  - Record the MAC address shown in the General tab in [Figure 3-5](#).

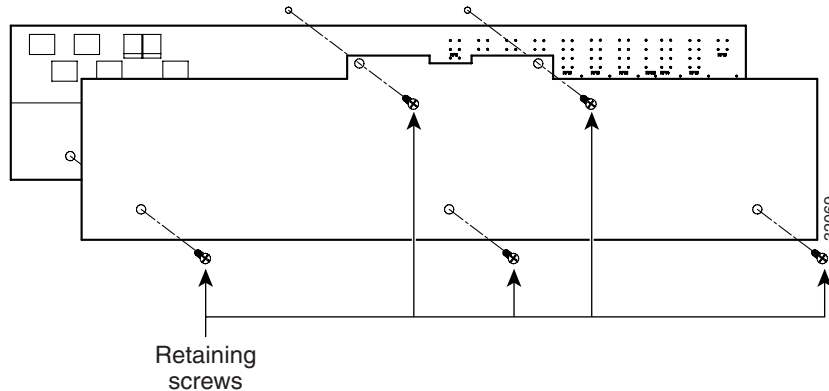
**Figure 3-5 Find the MAC address**



- 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**



- 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 (default login) view, click 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 (default login) view, right-click 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 (default login) view, right click 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** Log 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:

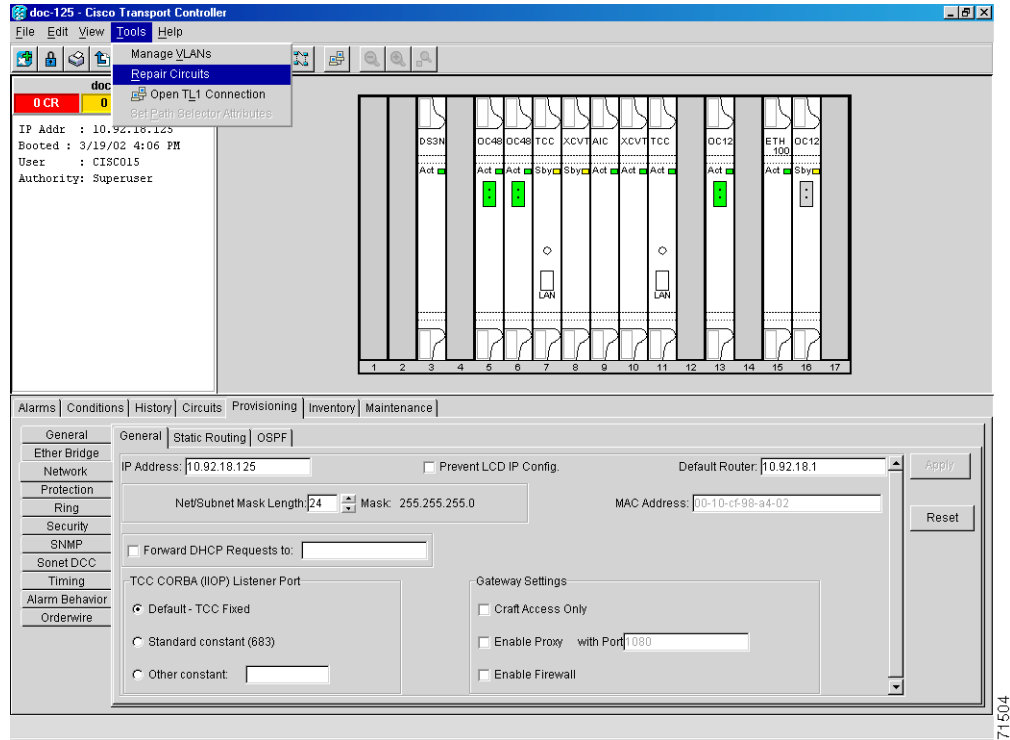
- a. In node (default login) view, click the **Provisioning > Network** tabs.
- b. Record the MAC address shown in the General tab.

**Step 21** In node (default login) view, click the **Circuits** tab. Note that all circuits listed are in an INCOMPLETE state.

**Step 22** In node (default login) view, choose **Tools** from the menu bar and click **Repair Circuits** (Figure 3-7). The Circuit Repair dialog box is displayed.

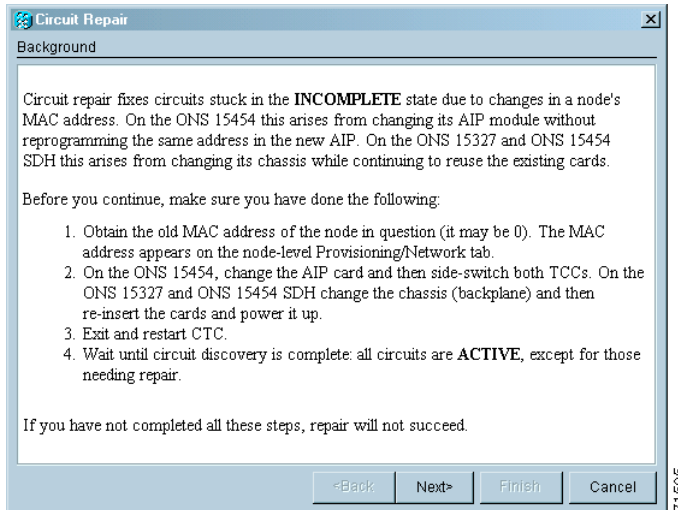


Figure 3-7 Repair Circuits in the Menu Bar

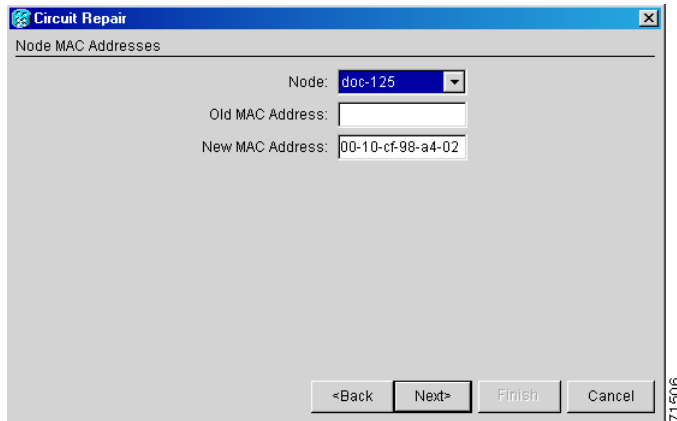


- Step 23** Read the instructions in the Circuit Repair dialog box (Figure 3-8). If all the steps in the dialog box have been completed, click **Next>**. Ensure you have the old and new MAC addresses.

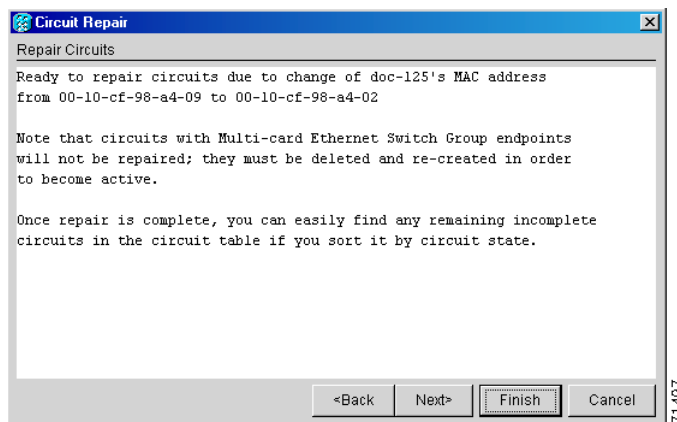
Figure 3-8 Repairing circuits



- Step 24** The Node MAC Addresses dialog box displays (Figure 3-9):
- From the Node pull-down menu, choose the name of the node where you replaced the AIP.
  - In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.
  - 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.

When the circuit repair is complete, the Circuits Repaired dialog box will display.

- Step 26** Click **OK**.
- Step 27** In the new node (default login) view, click 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 28** 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.

## 3.7 Replace the Electrical Interface Assembly

|                                |                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing EIA with a new EIA.                                                                                                              |
| <b>Tools/Equipment</b>         | <ul style="list-style-type: none"> <li>• #2 Phillips screwdriver</li> <li>• BNC insertion and removal tool (optional; for use with high-density BNC EIAs)</li> </ul> |
| <b>Prerequisite Procedures</b> | None                                                                                                                                                                 |
| <b>Required/As Needed</b>      | As needed                                                                                                                                                            |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                                               |

---

**Step 1** To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 3-6).

**Step 2** Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA 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.

---

**Step 5** Line up the connectors on the new EIA with the mating connectors on the backplane.

**Step 6** Gently push the EIA until both sets of connectors fit together snugly.

**Step 7** Replace the nine perimeter screws that you removed while removing the backplane cover.

**Step 8** If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

**Step 9** Reattach the lower backplane cover.

---

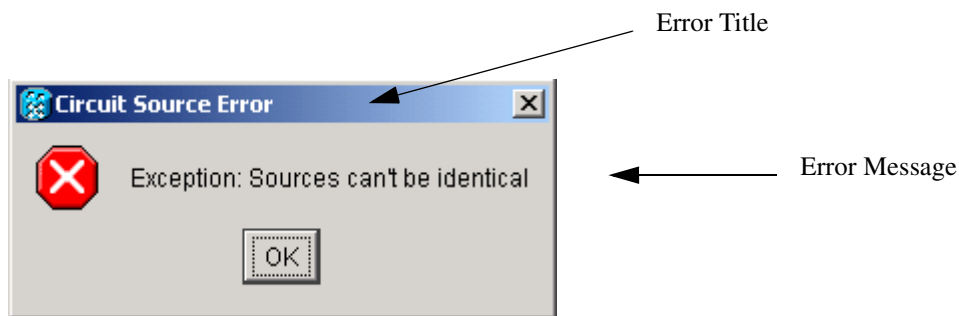




## Error Messages Troubleshooting

This chapter explains how to troubleshoot commonly-encountered error messages for the Cisco ONS 15454. The error dialogue consists of two parts: the error title and the error message.

**Figure 4-1** An error dialog box



Sections in this chapter are divided into error type (for example, circuit errors, BLSR errors, etc.) followed by the error title(s) for each dialog.

### 4.1 Circuit Errors

This section includes circuit-related error messages. The following headings show the error title (e.g. 4.1.x). If the same error title has multiple error messages, the error messages are listed as subheadings (e.g. 4.1.x.x)

#### 4.1.1 Circuit Source Error

The following messages appear in the Circuit Source Error dialog box. For detailed circuit creation instructions, refer to the *Cisco ONS 15454 Procedure Guide*.

##### 4.1.1.1 Exception: Source node must be selected

This error message appears if you click Next on the Circuit Source Creation dialog without entering a source node.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Choose the primary source node for the circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the primary source.
  - Step 4** Click **Next**.
- 

#### 4.1.1.2 Exception: Source is not fully specified

This error message is displayed when the source circuit is not fully defined.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Choose the primary source node for the circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the primary source.
  - Step 4** Click **Next**.
- 

#### 4.1.1.3 Exception: Secondary Source is not fully specified

This error message is displayed when the secondary circuit is not fully defined.

- 
- Step 1** Click **OK** to close the dialog.
  - Step 2** Choose the secondary source node for the circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the secondary source.
  - Step 4** Click **Next**.
- 

#### 4.1.1.4 Exception: Sources can't be identical

This error occurs if identical primary and secondary source circuits are selected.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Click the **Use Secondary Source** button.
  - Step 3** Choose a Slot, Port and STS or VT number, if applicable, that is not the same as the primary circuit.
  - Step 4** Click **Next**.
-

## 4.1.2 Circuit Destination Error

The following error messages appear in the Circuit Destination Error dialog box.

### 4.1.2.1 Exception: Destination node must be selected

This error message appears if you do not select a destination node and try to proceed to the next circuit creation screen.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Choose the primary destination node for the circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the primary destination.
  - Step 4** Click **Next**.
- 

### 4.1.2.2 Exception: Destination is not fully specified

This error message is displayed when the destination circuit is not fully defined.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Choose the primary destination node for circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the primary source.
  - Step 4** Click **Next**.
- 

### 4.1.2.3 Exception: Secondary Destination is not fully specified

This error message is displayed when the secondary destination circuit is not fully defined.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Choose the secondary destination node for the circuit.
  - Step 3** Choose the Slot, Port, STS and VT if applicable for the secondary destination.
  - Step 4** Click **Next**.
- 

### 4.1.2.4 Exception: Destinations can't be identical

This error occurs if when primary and secondary circuit destinations are selected.

- 
- Step 1** Click **OK** to close the error dialog.
  - Step 2** Click the "Use Secondary Destination" button.
  - Step 3** Choose a Slot, Port and STS or VT number if applicable that is not the same as the primary circuit.

**Step 4** Click **Next**.

---

## 4.1.3 Circuit Destroy Failed

The following messages appear in the Circuit Destroy Failed dialog box.

These errors occur when a circuit is being deleted and CTC loses DCC or gateway LAN communication to the node.

### 4.1.3.1 CmsCommFailException: < node-ip address > Communications error (COMM\_FAILURE) while attempting to set the CircuitModel.delete attribute

CTC cannot communicate to all the nodes in the network where the circuit must traverse. CTC must be able to communicate with all of the nodes before it is safe to delete the circuits.

---

- Step 1** Click **OK** to close the error dialog.
  - Step 2** Go to the network view and verify that none of the nodes are greyed out
  - Step 3** Click the **Alarms** tab.
  - Step 4** Search for alarms to indicate that there is a DCC termination failure.
  - Step 5** If a DCC termination failure is present, reprovision the DCC channel or check for a broken fiber between the two nodes.
  - Step 6** If a DCC termination failure is not present, access a command prompt from CTC and run the ping command to the nodes the circuit traverses. See the [“Ping the ONS 15454” procedure on page 1-48](#).
  - Step 7** Repeat Step 6 as needed to verify that CTC can successfully run the ping command to each of the nodes.
  - Step 8** Click the **Circuit** tab in either the network view or node view.
  - Step 9** Highlight the circuit that you need to delete.
  - Step 10** Click the **Delete** button.
  - Step 11** Click the **Yes** button when the circuit deletion warning dialogue appears.
  - Step 12** Delete as many circuits as necessary.
- 

### 4.1.3.2 CmsCommFailException: < node-ip address > The Node was not initialized while attempting to set the CircuitModel.delete attribute

CTC cannot communicate with all the nodes in the network where the circuit must traverse. CTC must be able to communicate with all of the nodes before it is safe to delete the circuits.

---

- Step 1** Click **OK** to close the error dialog.
- Step 2** Go to the network view and verify that none of the nodes are greyed out
- Step 3** Click the **Alarms** tab.
- Step 4** Search for an alarms to indicate that there is a DCC termination failure.



- 
- Step 5** If a termination failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes.
  - Step 6** If an SDCC termination failure is not present, run the ping command to the nodes the circuit traverses. See the [“Ping the ONS 15454” procedure on page 1-48](#).
  - Step 7** Verify that CTC can successfully run the ping command to each of the nodes.
  - Step 8** Click the **Circuit** tab in either the network or node view.
  - Step 9** Highlight the circuit that you want to delete.
  - Step 10** Click the **Delete** button.
  - Step 11** Click the **Yes** button when the circuit deletion warning dialogue appears.
  - Step 12** Delete as many circuits as necessary.
- 

## 4.1.4 Auto-Ranging Circuit Creation

The following messages appear in the Auto-Ranging Circuit Creation dialog box.

### 4.1.4.1 Unable to provision circuit Unexpected exception encountered Attempts to access a VtAdit that has been destroyed.CmsObjectNotExistException: Attempts to access a VtAdit that has been destroyed.

This error occurs when routing a group of VT circuits over an existing VT tunnel.

This error typically occurs when a CTC session attempts to access a VT-grooming STS Path that has been deleted by another CTC user (or session).

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Cancel the circuit dialogue.
  - Step 3** Restart the circuit dialogue.
  - Step 4** Continue to provision the original circuit.
- 

### 4.1.4.2 NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements.

This error occurs when CTC attempts to create auto-ranged circuits but it cannot provision a route for the subsequent circuits. One of the protection paths is fully blocked because there is no available bandwidth after the Nth circuit is attempted.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.

- One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
- A BLSR was along the path but there was no common time slot available in the ring.
- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
  - A node along the path from source to drop was "excluded" and no other path is available.
  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
  - One of the required links does not have bandwidth to support the circuit.
  - One of the required links for a path-protected circuit cannot be protected

If a circuit routing failure is encountered, identify the root cause of the problem among the above set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Calculate how much available bandwidth is available on both the working and the protection path by following the steps below.
- a. Go to the network view on the CTC.
  - b. Click on each span and then right-click the mouse button.
  - c. Click the **Circuits** label from the drop down screen. A table appears that shows the available bandwidth.
  - d. Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working and a protection path.
- Step 3** Click **Create** on the main circuit screen.
- Step 4** Input the number of available circuits based on the available bandwidth into the **Number of Circuits** box.
- Step 5** Click **Next** at the bottom of the screen.
- Step 6** Continue to provision both the source and destination circuits.
- Step 7** Click **Finish** on the Circuit Routing Preferences screen.
- 

### 4.1.4.3 Unable to drop route `ComputeRouteInMixedDomains: No Route found with given requirements NoRoute: ComputeRouteInMixedDomains: No Route found with given requirements`

This error is very similar to the previous error, but applies to drop circuits only. Both of the errors can occur when a path is no longer available.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.

- One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
- A BLSR was along the path but there was no common time slot available in the ring.
- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
  - A node along the path from source to drop was "excluded" and no other path is available.
  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
  - One of the required links does not have bandwidth to support the circuit.
  - One of the required links for a path-protected circuit cannot be protected

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Calculate how much available bandwidth is available on both the working and the protection path by following the steps below.
- a. Go to the network view on the CTC.
  - b. Click on each span and then right-click the mouse button.
  - c. Click the **Circuits** label from the drop down screen. A table appears that shows the available bandwidth.
  - d. Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working and a protection path.
- Step 3** Click **Create** on the main circuit screen.
- Step 4** Input the number of available circuits based on the available bandwidth into the **Number of Circuits** box.
- Step 5** Click **Next** at the bottom of the screen.
- Step 6** Continue to provision both the source and destination circuits.
- Step 7** Click **Finish** on the Circuit Routing Preferences screen.
- 

#### 4.1.4.4 NoRoute: Unable to route VT Circuit: possible reasons: 1) VT Tunnel required and cannot route due to XCs in the path from source to destination 2) Cannot find route that satisfies given requirements

This exception occurs if a one or more lower order (LO) tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Provision the LO circuit.
-

### 4.1.4.5 Exception: Source is not fully specified

This error occurs when more auto-ranged circuits than available ports or STSs are requested. For example, if a user attempts to automatically provision 15 DS3 circuits and there is only one 12-port DS3 card in the system, the error will appear after all 12 DS3 ports are utilized. The auto-ranging circuit provisioning does not automatically increment the slot for the source or destination. It does not automatically increment the port number on the OC-3 card for STS-1 circuits.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click **Back**.
  - Step 3** Provision more ports on the system to satisfy the available auto-ranging requirements.
  - Step 4** Insert additional cards if slots are available.
  - Step 5** The installed card should reflect the type of circuit that is being added (i.e. DS-3, DS-1, etc.)
  - Step 6** If more slots are unavailable, the number of auto ranged circuits must be reduced.
- 

## 4.1.5 Node Selection Error

The following message appears in the Node Selection Error dialog box.

### 4.1.5.1 Failure getting list of available ports from <node-name> <node ipaddress> Communications error (COMM\_FAILURE) while attempting to get the ConnectionModels.availEntitiesForVtsPath attribute.

This specific error occurred when DCC was taken down during the auto creation of VT circuits.

The general cause of the problem is loss of connectivity to one of the nodes in the network. Deletion of DCC is one of the specific reasons for loss of connectivity. Another reason might be IP routing failures due to static route reconfiguration.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to the network view and verify that none of the nodes are greyed out.
  - Step 3** Click the **Alarms** tab and search for alarms to indicate an SDCC failure.
  - Step 4** If an SDCC failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes, then continue provisioning the circuit.
  - Step 5** If an SDCC failure is not present, run the ping command to the nodes the circuit traverses. See the [“Ping the ONS 15454” procedure on page 1-48](#).
  - Step 6** Verify that CTC can successfully run the ping command to each of the nodes.
  - Step 7** Click the **Circuit** tab in either the network or node view.
  - Step 8** Click the **Create** button.
  - Step 9** Continue provisioning the circuit.

**Note**

During the auto creation process verify that the network is stable by watching for the greying out of nodes or SDCC alarm messages.

## 4.1.6 Circuit Creation Error

The following messages appear in the Circuit Creation Error dialog box.

### 4.1.6.1 Circuit creation cannot proceed due to changes in the network, which affect the circuit(s) being created. The dialog will close. Please try again.

This error message occurs if a network change occurs simultaneously to circuit provisioning.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to the network view and verify that none of the nodes are greyed out
  - Step 3** Click the **Alarms** tab and search for alarms that indicate an SDCC failure.
  - Step 4** If an SDCC failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes, then continue provisioning the circuit.
  - Step 5** If an SDCC failure is not present, run the ping command to the nodes the circuit traverses. See the [“Ping the ONS 15454” procedure on page 1-48](#).
  - Step 6** Verify that CTC can successfully run the ping command to each of the nodes.
  - Step 7** Click the **Circuit** tab in either the network or node view.
  - Step 8** Click the **Create** button.
  - Step 9** Continue provisioning the circuit.
- 

## 4.1.7 Error While finishing Circuit Creation

The following messages appear in the Error While Finishing Circuit Creation dialog box.

### 4.1.7.1 Unable to provision circuit No VT-capable STSs are available at <node-name>

The user can not proceed any further until some circuits are deleted. The maximum number of cross-connections that can be created on the ONS 15454 has been reached.

Each VT1.5 cross-connection takes up one slot in two or more VT-grooming STSs on the node.

Only 24 VT-grooming STSs are available at each node. Hence, the maximum number of VT1.5 cross-connections possible on a given node depends on the type of connections and the configuration. For example, if all cross-connections were simple 2-way type connections and all 24 STSs were fully packed, the maximum number is 336 (= 24\*28/2).

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to the node view and click the **Circuit** tab.
  - Step 3** Highlight some circuits that need to be deleted.
  - Step 4** Click the **Delete** button.
  - Step 5** Click on **Yes** when the warning dialogue appears.
  - Step 6** Create another circuit to replace the deleted circuit.



**Note** Remember, there is a finite number of cross connections that can be provisioned on the ONS 15454. To add more cross connections, existing cross connection must be deleted.

---

### 4.1.7.2 Unable to provision circuit **Circuit provision error Unable to create connection at <node-name>**

This error occurs when two users attempt to provision the same circuit simultaneously. The error message also occurs when connectivity is lost to the node being provisioned during circuit creation.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Delete the created circuit.
  - Step 3** Coordinate with the other user when provisioning circuit across the same equipment.
- 

### 4.1.7.3 NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements.

This error occurs when CTC cannot provision a route for auto-ranged circuits.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Free up some available bandwidth on the blocked path or route the circuit along an unprotected path with some available bandwidth. To determine the available bandwidth:
    - a. Go to the network view.
    - b. Click each span and then right-click the mouse button.
    - c. Click the **Circuits** label from the drop down screen. A table will appear that shows the available bandwidth.
    - d. Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.
  - Step 3** Click **Create** on the main circuit screen.
  - Step 4** Input the circuit attributes - Name, Type, Size.
  - Step 5** Click **Next**.

**Step 6** Continue to provision both the source and destination circuits.

---

#### 4.1.7.4 Circuit sanity check failed. Invalid connection at node <node name> SanityCheckFailed: Invalid connection at node <node name>.

The error message appears if a UPSR connection cannot be created due to a protected source or destination endpoint.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click **Back**.
  - Step 3** Unclick **Use Secondary Destination**.
  - Step 4** Click **Back**.
  - Step 5** Unclick **Use Secondary Source**.
  - Step 6** Click **Next**.
  - Step 7** Choose the same node for the destination circuit as is chosen for the source circuit.
  - Step 8** Choose destination slot, port, STS and VT parameters for both the primary and secondary circuits.
  - Step 9** Click **Finish**.
- 

#### 4.1.7.5 CmsObjectNotExistException: Attempt to access the CtAuditModel.getAvailableSts attribute for an object that does not exist.

This error occurs when a user attempts to access a VT-grooming STS Path that has been deleted by another user. Reattempt the circuit provisioning after canceling out the circuit dialogue.

#### 4.1.7.6 Circuit spans verification: selected spans are invalid! Invalid span combination at Node <node name> SanityCheckFailed: Invalid span combination at Node <node name>

This error message is related to the validity of the input and output paths at each circuit node that result from the selection of spans during manual routing.



**Note**

Circuit sources and drops are also considered paths, but it is the selection of spans that occurs during manual routing. The sources and drops are fixed during this phase of circuit creation.

---

Like the "Invalid connection at node <node name>" error message, it identifies invalid situations where a selector path of a UPSR selection has line-level protection. The selector paths are circuit spans rather than source or destination endpoints.

---

- Step 1** Click **OK** to clear the error dialog.
- Step 2** Choose additional spans from source node to the destination node.
- Step 3** Choose a second span if the circuit is to be path protected from source node to destination node.

**Step 4** Click **Finish**.

---

#### 4.1.7.7 Circuit spans verification" selected spans are invalid! Link Diverse Path requirement is not met. The link is <node name source -> <node name destination> (LINK\_VTT unprot, State=Up). Node Check is the link is a VT Tunnel

This error occurs if link diversity is requested for a VT circuit and the tunnels selected do not traverse different paths.

---

**Step 1** Click **OK** to clear the error dialog.

**Step 2** Go to the "Route Review and Edit" screen.

**Step 3** Select one of the spans that traverses a tunnel.

**Step 4** Click **Remove**.

The span should disappear on the screen.

**Step 5** Click a span that does not follow the original tunnels path.

**Step 6** Continue to route the circuit path to the destination node by selecting and adding all the necessary spans in the path.

**Step 7** Click **Finish**.

---

#### 4.1.7.8 Circuit sanity check failed. Path specified is not protected. Check span <node name> -> <nodename> (LINK\_PHYSICAL unprot, State=Up). OCN IsmState=2,2.

This error message appears when a protection path is not provisioned for a manually-routed circuit.



**Note**

An alternative solution is to create line protection (1+1) from source to destination; in this case, a protection path would be inherently included in the circuit route.

---

**Step 1** Click **OK** to clear the error dialog.

**Step 2** Choose a second span from source node to destination node.

**Step 3** Click **Finish**.

---

#### 4.1.7.9 Circuit sanity check failed. Source/Drop is an endpoint of a network link.

This error message occurs when the user attempts to create a circuit from one trunk side to another trunk side and does not use a dropped circuit.

This error occurs if the source or destination is a trunk endpoint.

---

**Step 1** Go to the Circuit Creation screen.



- Step 2** Choose circuit name, type and size.
  - Step 3** On the circuit source screen provision an STS from the trunk card (e.g the OC-48 supporting the ring).
  - Step 4** On the circuit destination screen provision an STS from the trunk card.
  - Step 5** Click **Finish**.
  - Step 6** Click **OK** to clear the error dialog.
  - Step 7** Go back and choose only drop side circuits.
- 

#### 4.1.7.10 Unable to route drop. ComputerRouteInMixedDomains: No Route found with given requirements. NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements

This error occurs when no available route around the ring is available. For example, one of the required links for a path-protected circuit cannot be protected. If a circuit routing failure is encountered, identify the root cause of the problem among the following set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
  - The network topology has not been fully discovered.
  - Sufficient network bandwidth is not available to support the requested circuit.
  - Path protection was requested and there is no end-to-end protected path available.
  - One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
  - A BLSR was along the path but there was no common time slot available in the ring.
  - The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
    - A node along the path from source to drop was "excluded" and no other path is available.
    - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
    - One of the required links does not have bandwidth to support the circuit.
- 

- Step 1** Click **OK** to clear the error dialog.
- Step 2** Go to the network view.
- Step 3** Click each span and then right-click the mouse button.
- Step 4** Click the **Circuits** label from the drop down screen.  
A table will appear which shows the available bandwidth.
- Step 5** Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.
- Step 6** Click **Create** on the main circuit screen.
- Step 7** Provision the circuit attributes (Name, Type, Size).
- Step 8** Click **Next**.

- Step 9** Continue to provision both the source and destination circuits.
- 

## 4.1.8 Error Adding Drop

The following messages appear in the Error Adding Drop dialog box.

### 4.1.8.1 SanityCheckFailed: Source/Drop is an endpoint of a network link

This error occurs during one-way circuit provisioning when an additional drop to a trunk or network port is attempted.

- 
- Step 1** Go to the Circuit Creation screen.
- Step 2** Choose the circuit name, type, and size.
- Step 3** Uncheck the **Bidirectional** circuit box.
- Step 4** Choose an unprotected source and destination circuit between two spans.
- Step 5** Go back and highlight the original circuit.
- Step 6** Click **Edit**.
- Step 7** Click the **Drop > Create** tabs.
- Step 8** Add a circuit on the trunk of network side.
- Step 9** Click **OK** to clear the error dialog.
- Step 10** Choose a circuit that is on the drop side (not on the trunk side).
- 

### 4.1.8.2 Exception: Drop node must be selected

This error occurs when the drop node is not selected.

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Choose a node to drop the circuit.
- Step 3** Choose slot, port, STS, and VT if applicable.
- Step 4** Click **OK**.
- 

### 4.1.8.3 Circuit provisioning error Unable to add output to connection at <node-name> Path already in use

This error occurs when two CTC sessions are simultaneously provisioning circuits using the same path.

- 
- Step 1** Click **OK** to clear the error dialogue.
- Step 2** Coordinate with the operator attempting to provision a circuit on the same path.

**Step 3** Recreate the circuit.

---

## 4.1.9 Error Applying Changes

The following message appears in the Error Applying Changes dialog box.

### 4.1.9.1 InvalidProtectionOp: Unable to switch. A higher priority request may be present.

This error occurs when a user attempts to activate a UPSR switch and another user has already put a higher priority request already in place.

**Step 1** Click **OK** to clear the error dialogue.

**Step 2** Choose **Clear**.

**Step 3** Click **Apply**.

**Step 4** Choose new switch command.

**Step 5** Click **Apply**.

---

## 4.1.10 Error Deleting Circuit Drop

The following messages appear in the Error Deleting Circuit Drop dialog box.

### 4.1.10.1 IncorrectCircuitState: Circuit drop can be deleted only when state is CREATING, ACTIVE or DROP\_PENDING

This error occurs if the user attempts to delete dropped circuits that are not in the correct state.

**Step 1** Click **OK** to clear the error dialog.

**Step 2** Click the **Delete** button again after circuits are in the proper state.



**Note**

Circuits can only be deleted when they are in the proper state.

---

### 4.1.10.2 CannotDeleteLastDrop: Last circuit drop cannot be deleted. Please destroy the circuit instead

This error occurs when deleting a group of dropped circuits and one circuit is left which represents the original circuit. The circuit must be deleted from the main circuit screen.

**Step 1** Click **OK** to clear the error dialog.

---

**Step 2** Go to the main circuit screen and delete the circuit.



**Note**

The user can not delete the entire circuit from the drop screen. To delete the entire circuit, the user must go to the main circuit provisioning screen and then delete the circuit.

## 4.1.11 Error

The following circuit-related messages appear in the Error dialog box. (See also the “[Error](#)” section on [page 4-22](#) for BLSR-related messages that appear in this dialog box.)

### 4.1.11.1 Please select a node first

This error occurs when the user attempts to select a path while manually routing a circuit and a source node is not selected.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click on source node.
  - Step 3** Select only paths with a green arrow.
  - Step 4** Continue routing the circuit.
- 

### 4.1.11.2 This link may not be included in the required list. Constraints only apply to the primary path.

This error occurs during automatic circuit provisioning when the user checks Using Required Nodes/Spans and Nodal Diversity and the Required list contains only one route. The second protection route is automatically created.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Choose only one primary path.
  - Step 3** Click **Finish**.
- 

### 4.1.11.3 This node is not selectable: Only the Source node and nodes attached to included (blue) are selectable. Selecting a selectable node will enable its available outgoing spans

This error occurs when the a non-source node is selected in the manual routing area.

**Note**

Apart from the source node, it is also valid to select nodes attached to the spans that are already selected for this circuit. This error will appear if you select any other node.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click the source node.
  - Step 3** Click an available span designated by a green arrow.
  - Step 4** Click **Add Span**.
  - Step 5** Click the next span in sequence towards the green arrow.
  - Step 6** Click **Add Span**.
  - Step 7** If this is a protected span, complete a second protection path.
  - Step 8** Click **Finish**.
- 

#### 4.1.11.4 This span is not selectable. Only green spans with arrows.

This error appears when selecting a manual route that has a green line and not a green arrow.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go back and choose only green arrows.
- 

#### 4.1.11.5 Sorry, no paths are available on this link. Please make another selection.

This error occurs when a user selects an unavailable path for a manually-routed circuit.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Reroute the circuit around a path with available bandwidth.
  - Step 3** Click **Finish**.
- 

#### 4.1.11.6 This link may not be included in the required list. Only 1 outgoing link may be included for each node.

This error occurs when the user checks Using Required Nodes/Spans while provisioning an automatically-routed circuit. The circuit is setup to be unprotected. The required list can contain only one route.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Do not click on more than one link from the source.

- Step 3** Complete the circuit to the destination by selecting the remaining link.
- 

## 4.1.12 Circuit Deletion Error

The following message appears in the Circuit Deletion Error dialog box.

### 4.1.12.1 DeletionError: Following Circuits Could Not Be Scheduled for Deletion . Error deleting circuit TUN\_<node name> ::10:cerent.cms.ncp. SanityCheckFailed: VT Tunnel is in use.

The error occurs when the user tries to delete a VT tunnel before deleting the VT circuit.



**Note**

More than one VT circuit may be using the same VT tunnel; all circuits must be deleted before the tunnel can be deleted.

---

- Step 1** Click **OK** to clear the error dialog.
- Step 2** Highlight the VT circuit in the VT tunnel on the circuit screen.
- Step 3** Click the **Delete** button.
- Step 4** Highlight the VT tunnel on the circuit screen.
- Step 5** Click the **Delete** button.
- 

## 4.1.13 Circuit Attributes Error

The following messages appear in the Circuit Attributes Error dialog box.

### 4.1.13.1 Exception: Circuit name is too long(max 48)

This error occurs when a circuit name is assigned more than 48 characters.



**Note**

For auto-ranged circuits, the maximum circuit-name length is 43 characters.

---

- Step 1** Click **OK** to clear the error dialog.
- Step 2** Enter a circuit name that is less than or equal to 48 characters.
- Step 3** Click **Next**.
- 

### 4.1.13.2 NumberFormatException

This error occurs after clearing the Inter-domain Service Level value and proceeding to the next screen.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Enter the Inter-domain Service Level value using a positive integer.
  - Step 3** Click **Next**.
- 

### 4.1.13.3 NumberFormatException:99999999999999

This error occurs if the Inter-domain Service Level value is too large.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Enter the proper Inter-domain Service Level value.
  - Step 3** Click **Next**.
- 

### 4.1.13.4 Exception: Number of Circuit must be a positive integer

This error occurs if the Number of Circuits value is too large, is not an integer, or is left blank.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Clear the Number of Circuits box.
  - Step 3** Enter a smaller circuit ranging number.
- 

## 4.1.14 Error Validating Slot Number

The following message appears in the Error Validating Slot Number dialog box.

### 4.1.14.1 Please enter a valid value for the Slot Number

This error occurs if a bad slot number is applied to the circuit filter tool.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Enter a valid slot number.
  - Step 3** Click **OK**.
- 

## 4.1.15 Error Validating Port Number

The following message appears in the Error Validating Port Number dialog box.

### 4.1.15.1 Please enter a valid value for the Port Number

This error occurs if a bad port number is applied to the circuit filter tool.

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Enter a valid port number.
- Step 3** Click **OK**.
- 

## 4.1.16 Circuit Route Constraints Error

The following message appears in the Circuit Route Constraints Error dialog box.

### 4.1.16.1 Unable to route drop Compute. RouteInMixedDomains: No Route found with given requirements. NoRoute: ComputeRouteInMixedDomains: No Route found with given requirements.

This error occurs when circuit routing fails; a path is no longer available. This error applies to drop circuits only.

If a circuit routing failure is encountered, identify the root cause of the problem among the following set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.
- One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
- A BLSR was along the path but there was no common time slot available in the ring.
- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
  - A node along the path from source to drop was "excluded" and no other path is available.
  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
  - One of the required links does not have bandwidth to support the circuit.

- 
- Step 1** Click **OK** to clear the error dialog.
- Step 2** Go to the network view.
- Step 3** Click each span and then right-click the mouse button.
- Step 4** Click the **Circuits** label from the drop down screen.
- A table will appear which shows the available bandwidth.



- Step 5** Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.
  - Step 6** Click **Create** on the main circuit screen.
  - Step 7** Provision the circuit attributes (Name, Type, Size).
  - Step 8** Click **Next**.
  - Step 9** Continue to provision both the source and destination circuits.
- 

## 4.2 BLSR Errors

This section includes BLSR-related error messages. The following headings (4.2.x) show the error title. If the same error title has multiple error dialogues, the error dialogues are listed as subheadings.

### 4.2.1 Cannot Delete Ring

The following message appears in the Cannot Delete Ring dialog box.

#### 4.2.1.1 There is a protection operation set. All protection operations must be clear for ring to be deleted.

This error occurs while a BLSR switch is active and the user attempts to delete the ring.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click the **Conditions** tab.
  - Step 3** Double-click the target ring (the ring you will delete) to display the BLSR Edit Window.
  - Step 4** The following protection switches are possible: Lockout Span, Force Ring, Force Span, Manual Ring, Manual Span, Exercise Ring, and Exercise Span. These can be identified by the letters L, F, M, and E inside the port. Find a port on the edit map with one of these letters present.
  - Step 5** Right-click the port and select **set East/West protection op.**
  - Step 6** Select **Clear** and click **OK**.
  - Step 7** Click **Yes** on the "Confirm BLSR Operation" dialog.
  - Step 8** Return to the BLSR Provisioning tab in the network view.
  - Step 9** Reattempt to delete the ring.
- 

### 4.2.2 Invalid Ring ID

The following message appears in the Invalid Ring ID dialog box.

### 4.2.2.1 RingID must be an integer between 0 and 9999

This error occurs if a Ring ID greater than 9999 is selected in the BLSR configuration wizard. This error can also occur if a negative number or sequence of alpha characters is entered.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Enter a Ring ID between 0 and 9999.
  - Step 3** Click **Next**.
- 

## 4.2.3 Error

The following messages appear in the Error dialog box.

### 4.2.3.1 The Ring ID value is not valid . Please enter a valid number between 0 and 9999.

This error occurs if a BLSR Ring ID is changed to a number greater than 9999 or a string of alpha characters.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Enter a Ring ID between 0 and 9999
  - Step 3** Click **Apply**.
  - Step 4** Click **OK** when the “Are you sure?” dialogue appears.
- 

### 4.2.3.2 Cannot set reversion to INCONSISTENT!

This error occurs if INCONSISTENT is selected in the BLSR wizard.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Choose a reversion time between .5 and 12 minutes, or choose “never.”
  - Step 3** Click **Apply**.
- 

### 4.2.3.3 You must enter a number and it must be between 0 and 31.

This error occurs in the BLSR wizard edit screen when the node ID entered is not between 0 and 31.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click **Cancel** to close the Edit ID window.
  - Step 3** Examine the BLSR wizard edit window to determine the node IDs in the ring. The node ID is the number in parentheses next to the node name in the edit map.

- Step 4** Right-click the node whose ID you wish to change and select **Set Node ID**.
  - Step 5** Enter a node ID between 0-31 that is not already in use.
  - Step 6** Click **OK**..
- 

#### 4.2.3.4 Error - this node ID is already in use. Please choose another.

This error occurs if the user chooses a duplicate node ID.

---

- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Click **Cancel** to close the Edit ID window.
  - Step 3** By examining the BLSR wizard edit window determine the node IDs in the ring. The node ID is the number in parentheses next to the node name in the edit map.
  - Step 4** Right-click the node with the node ID you need to change and select **Set Node ID**.
  - Step 5** Enter a node ID between 0-31 that is not already in use.
  - Step 6** Click **OK**..
- 

## 4.2.4 Error Applying Changes

The following messages appear in the Error Applying Changes dialog box.

### 4.2.4.1 Exception: Unable to switch East Line, a higher priority request may be present.

This error occurs when an existing request is present and a lower order request is attempted.

---

- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to the East Switch BLSR box and choose a switch of equal or higher priority than the switch in the West Switch BLSR box.
  - Step 3** Go to the network view.
  - Step 4** Click the **Provisioning > BLSR** tabs.
  - Step 5** In the edit map double-click on the BLSR.
  - Step 6** Identify the port in the ring with a protection operation. The port will have an L, F, M, or E present.
  - Step 7** Right-click the port, clear the protection operation, and click **OK**.
  - Step 8** Right-click the desired port, change the protection operation, and click **OK**.
- 

### 4.2.4.2 Exception: Unable to switch West Line, a higher priority request may be present.

This error occurs when an existing request is present and a lower order request is attempted.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to the West Switch BLSR box and choose a switch of equal or higher priority than the switch in the East Switch BLSR box.
  - Step 3** Go to the network view.
  - Step 4** Click the **Provisioning > BLSR** tabs.
  - Step 5** In the edit map double-click on the BLSR.
  - Step 6** Identify the port in the ring with a protection operation. The port will have an L, F, M, or E present.
  - Step 7** Right-click the port, clear the protection operation, and click **OK**.
  - Step 8** Right-click the desired port, change the protection operation, and click **OK**.
- 

## 4.2.5 Duplicate Node ID

The following message appears in the Duplicate Node ID dialog box.

### 4.2.5.1 New Node ID (N) for Ring ID N duplicate ID of node <ip address>

This error occurs when an existing node ID is selected from the BLSR provisioning screen.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Go to one of the nodes in the ring.
  - Step 3** Click the **Provisioning > BLSR** tabs.
  - Step 4** Click the **Ring Map** button.
  - Step 5** Observe the node ID numbers in the ring map table.
  - Step 6** Choose a node ID number between 0 and 31 that is not already in use.
  - Step 7** Click **Apply**.
- 

## 4.2.6 BLSR Error

The following messages appear in the BLSR Error dialog box.

### 4.2.6.1 Exception: West and East ports must be different

This error occurs if a BLSR is provisioned to use the same slot for both the east and west lines.

- 
- Step 1** Click **OK** to clear the error dialog.
  - Step 2** Make sure the West Line and the East line are not using the same slot.

**Step 3** Click **OK**.

---

### 4.2.6.2 Exception: West and East ports must have the same line rate

This error occurs if a BLSR is provisioned using different line rates for the east and west lines.

---

**Step 1** Click **OK** to clear the error dialog.

**Step 2** Make sure the West Line and the East line are not using different line rates.

**Step 3** Click **OK**.

---

### 4.2.6.3 Exception: Unable to parse Ring ID

This error occurs if a bad value is chosen when provisioning a BLSR span, such as an alpha character, a number that is too large, or no number at all.

---

**Step 1** Click **OK** to clear the error dialog.

**Step 2** Enter a ring ID between 0 and 9999

**Step 3** Click **OK**.

---





---

## A

AIC card (EXT alarm) [2-50](#)  
AIP [2-91](#)  
    different cover types [2-90](#)  
    MEA [2-89](#)  
    MFGMEM alarm [2-93](#)  
    replace [3-13](#)  
air filter, replace [3-5](#)  
AIS [2-16](#)  
AIS-L [2-16](#)  
AIS-P [1-67, 2-16](#)  
AIS-V [1-65, 2-17](#)  
alarms  
    alarms are indexed individually by name  
    alphabetical list [2-4](#)  
    list of critical alarms [2-1](#)  
    list of major alarms [2-2](#)  
    list of minor alarms [2-2](#)  
    TL1 [2-1](#)  
alarm troubleshooting [2-1 to 2-134](#)  
AMI coding [2-73, 2-74](#)  
APSB [2-18](#)  
APSCDFLTK [2-18](#)  
APSC-IMP [2-19](#)  
APSCINCON [2-20](#)  
APSCM [2-20](#)  
APSCNMIS [2-21](#)  
APSM [2-22](#)  
APS see protection switching  
ARP [1-60](#)  
asynchronous mapping [2-98](#)  
AUTOLSROFF [2-24](#)

automatic protection switching  
    byte failure [2-18](#)  
    channel failure on protect card [2-64](#)  
    channel mismatch [2-20](#)  
    inconsistent code [2-20](#)  
    invalid k bytes [2-19](#)  
    mode mismatch failure [2-22](#)  
    ring switch failure [2-53](#)  
    span switch failure [2-55](#)  
    UPSR alarms [2-25, 2-26](#)  
    UPSR revertive switch occurred [2-27](#)  
    UPSR switch (condition) [2-25, 2-26](#)  
automatic protection switching see protection switching  
automatic reset [2-25](#)  
AUTORESET [2-25](#)  
AUTOSW-AIS [2-25](#)  
AUTOSW-LOP (STSMON) [2-25](#)  
AUTOSW-LOP (VT-MON) [2-26](#)  
AUTOSW-PDI [2-26](#)  
AUTOSW-SDBER [2-26](#)  
AUTOSW-SFBER [2-26](#)  
AUTOSW-UNEQ (STSMON) [2-27](#)  
AUTOSW-UNEQ (VT-MON) [2-27](#)

---

## B

B8ZS [2-73, 2-74](#)  
battery  
    low voltage alarm [2-44](#)  
BER  
    SD-P condition [2-106](#)  
    SF-L condition [2-107](#)  
    SFP condition [2-108](#)

- verify threshold level [2-133](#)
  - bit error rate see BER
  - BITS
    - daisy-chained [1-69](#)
    - errors [1-68](#)
    - holdover timing [1-69](#)
    - loss of frame [2-73](#)
    - loss of signal [2-79](#)
  - BKUPMEMP [2-27](#)
  - BLSR
    - far-end protection line failure [2-64](#)
    - force switch condition [2-111](#)
    - improper configuration (alarms) [2-18](#)
    - lockout condition [2-72](#)
    - manual ring switch condition [2-104, 2-105](#)
    - manual span condition [2-89](#)
    - ring mismatch [2-104](#)
    - ring switch failure [2-54](#)
    - span lockout on working or protect [2-72](#)
    - squelch alarm [2-111](#)
  - BLSROSYNC [2-28](#)
  - BNC connector [2-101, 2-123](#)
  - browser
    - applet security restrictions [1-53](#)
    - cannot launch Java [1-46](#)
    - stalls during download [1-50](#)
- 
- C**
- cache, redirect Netscape cache [1-51](#)
  - CARLOSS
    - cause of TPTFAIL [2-122](#)
    - equipment [2-28](#)
    - E series Ethernet [2-29](#)
    - G1000-4 card [2-31](#)
  - carrier loss [2-29, 2-31](#)
  - CBIT framing [1-22](#)
  - circuits
    - AIS-V alarm on DS3XM-6 card [1-65](#)
    - circuit state transition error [1-64](#)
    - delete [2-132](#)
    - identify circuit state [1-65](#)
    - identify failure points [1-4, 1-22](#)
    - troubleshooting [1-4](#)
    - VT1.5 creation error [1-66](#)
  - CLDRESTART [2-33](#)
  - COMIOXC [2-34](#)
  - CONCAT [2-35](#)
  - conditions indexed individually by name
  - CONTBUS-A-18 [2-35](#)
  - CONTBUS-B-18 [2-36](#)
  - CONTBUS-IO-A [2-37](#)
  - CONTBUS-IO-B [2-38](#)
  - cross-connect cards
    - main payload bus failure [2-40](#)
    - reset [2-39](#)
    - switching matrix failure [2-116](#)
    - test [1-9, 1-15](#)
    - XC10G incompatibility with backplane [2-89](#)
  - CTC
    - applet not loaded [1-46](#)
    - applet security restrictions [1-53](#)
    - delete cache files [1-52](#)
    - grey node icon [1-53](#)
    - list of alarms [2-1](#)
    - log in [3-2](#)
    - log-in errors [1-46, 1-50, 1-53, 1-56](#)
    - loss of TCP/IP connection [2-28](#)
    - release interoperability problems [1-56](#)
    - username and password mismatch [1-56](#)
    - verifying PC connection [1-48](#)
  - CTNEQPT-PBPROT [2-39](#)
  - CTNEQPT-PBWORK [2-40](#)
  - cyclic redundancy checking (CRC) [2-27](#)
- 
- D**
- database memory exceeded [2-42](#)



- DATAFLT [2-42](#)
  - DCC
    - channel loss [2-44](#)
    - connection loss [1-57](#)
    - create or verify DCC terminations [2-130](#)
    - delete a DCC termination [2-70](#)
    - disable autodiscovery [3-2](#)
    - limitations with OC-3 [1-68](#)
  - default K alarm [2-18](#)
  - DISCONNECTED [1-48](#)
  - DS-3 card
    - AIS-P not reported from external equipment [1-67](#)
    - loss of frame [2-62](#)
    - loss of signal [2-63](#)
  - DS3-MISM [2-42](#)
  - DS3XM-6 card
    - AIS-V alarm and unused VT circuits [1-65](#)
    - FEAC features [1-21](#)
    - incomplete circuit from DS-3 card [1-67](#)
    - loopback command initiated [2-85](#)
  - DS-N cards
    - facility loopback example [1-2](#)
    - failure to switch [2-51](#)
    - frame format mismatch [2-42](#)
    - identify points of failure on circuit path [1-4](#)
    - idle DS-3 signal [2-61](#)
    - line alarms [2-127](#)
    - LOF [2-74](#)
    - loopback facility alarm [2-85](#)
    - loopback signal received [2-85](#)
    - loss of signal [2-79, 2-80](#)
    - reset [2-134](#)
    - terminal loopback alarm [2-87](#)
    - test [1-6, 1-19, 1-24](#)
    - LOF [2-75](#)
    - loopback facility alarm [2-85](#)
    - LOS [2-81](#)
    - terminal loopback condition [2-87](#)
  - EHIBATVG-A [2-43](#)
  - EHIBATVG-B [2-43](#)
  - EIAs
    - facility loopback test [1-2, 1-5](#)
    - replace [3-19](#)
    - test [1-7, 1-20](#)
  - electrical cabling [1-6](#)
  - ELWBATVG-A [2-43](#)
  - ELWBATVG-B [2-44](#)
  - EOC [2-44](#)
  - EQPT [2-46](#)
    - BKUMEMP [2-27](#)
    - MISS [2-47](#)
  - equipment failure [2-57](#)
    - far-end DS-1 failure [2-57](#)
    - far-end DS-3 failure [2-58, 2-59](#)
    - hardware failure on reporting card [2-46](#)
    - missing fan-tray assembly [2-47](#)
  - error messages
    - BLSR-related [4-21](#)
    - circuit-related [4-1](#)
    - path in use [1-58](#)
  - Ethernet
    - carrier loss [2-29, 2-31](#)
    - configuring VLANs [1-62](#)
    - connectivity problems [1-59](#)
    - replace faulty GBIC [1-73](#)
    - Tag/Untag port connectivity [1-60](#)
    - troubleshooting connections [1-59](#)
  - Ethernet see also G1000-4 card
  - E-W-MISMATCH [2-47](#)
  - EXCCOL [2-49](#)
  - excess collisions [2-49](#)
  - EXERCISE-RING-REQ [2-49](#)
  - EXERCISE-SPAN-REQ [2-50](#)
- 
- E**
- east/ west mismatch alarm [2-47](#)
  - EC1-12 card

EXT [2-50](#)  
 EXTRA-TRAF-PREEMPT [2-50](#)

---

## F

facility loopback

- clear [1-6, 1-7](#)
- definition [1-2](#)
- DS-N card [1-23](#)
- intermediate node [1-28](#)
- source DS-N port [1-4](#)
- test a destination DS-N card [1-17](#)
- test a source DS-N port [1-4](#)
- test the circuit [1-5, 1-24](#)

FAILTOSW [2-51](#)

FAILTOSW-PATH [2-51](#)

FAILTOSWR [2-53](#)

FAILTOSWS [2-55](#)

FAN [2-55](#)

fan-tray assembly

- MEA [2-93](#)
- missing unit alarm [2-47](#)
- reset [2-134](#)

FEAC [1-21 to 1-22](#)

FEAC, alarms [1-22](#)

FE-AIS [2-56](#)

FE-DS1-MULTLOS [2-56](#)

FE-DS1-NSA [2-57](#)

FE-DS1-SA [2-57](#)

FE-DS1-SNGLLOS [2-58](#)

FE-DS3-NSA [2-58](#)

FE-DS3-SA [2-59](#)

FE-EQPT-NSA [2-59](#)

FE-EXERCISING-RING [2-60](#)

FE-EXERCISING-SPAN [2-60](#)

FE-FRCDWKSWPR-RING [2-60](#)

FE-FRCDWKSWPR-SPAN [2-61](#)

FE-IDLE [2-61](#)

FE-LOCKOUTOFPR-SPAN [2-62](#)

FE-LOF [2-62](#)

FE-LOS [2-63](#)

FE-MANWKSWPR-RING [2-63](#)

FEPRLF [2-64](#)

fiber and cabling errors [1-70](#)

fiber-optic connections [1-71](#)

flash manager [2-27](#)

flow rate [2-49](#)

FORCED-REQ [2-65](#)

frame format [2-42](#)

FRCDSWTOINT [2-65](#)

FRCDSWTOPRI [2-66](#)

FRCDSWTOSEC [2-66](#)

FRCDSWTOTHIRD [2-66](#)

free run synchronization [2-66](#)

FRNGSYNC [1-69, 2-66](#)

FSTSYNC [2-67](#)

FULLPASSTHR-BI [2-67](#)

---

## G

G1000-4 card

- alarms [2-122](#)
- CARLOSS alarm [2-31](#)
- LPBKTERMINAL [2-87](#)

GBIC [1-73](#)

---

## H

hairpin circuit

- create on destination node [1-14](#)
- create on source node [1-8](#)
- definition [1-3](#)
- perform on destination node [1-14](#)
- perform on source node [1-8](#)
- test hairpin loopback [1-9, 1-15](#)

hard reset (card pull) [3-4](#)

hardware replacement compatibility [3-9](#)

HITEMP [2-67](#)  
 HLDOVERSYNC [1-69](#)  
 HLDOVRSYNC [2-68](#)

---

## I

idle signal condition [2-61](#)  
 improper card removal [2-69](#)  
 IMPROPRMVL [2-69](#)  
 INC-ISD [2-70](#)  
 INCOMPATIBLE-SW [1-56](#)  
 INHSWPR [2-70](#)  
 INHSWWKG [2-71](#)  
 Internet Explorer [1-40, 3-2](#)  
 interoperability [1-56](#)  
 INVMACADR [2-71](#)  
 IP  
   connectivity [1-57](#)  
   designing subnets [1-58](#)  
   select address for log in [3-2](#)

---

## J

Java  
   browser will not launch [1-46](#)  
   Java Runtime Environment [1-54](#)  
 JRE  
   description [1-55](#)  
   incompatibility [1-54](#)  
   launch failure [1-46](#)

---

## K

KB-PASSTHR [2-72](#)  
 k bytes [2-18, 2-19, 2-72](#)

---

## L

lamp test [1-80](#)  
 LAN (CAT-5) cable [1-75](#)  
 LED  
   blinking STAT LED [1-70](#)  
   test [1-80](#)  
 line coding [2-68, 2-73](#)  
 line framing [2-73, 2-74](#)  
 line interface unit [1-2](#)  
 LKOUTPR-S [2-72](#)  
 lockout  
   clear a BLSR lockout [2-130](#)  
   clear a USPR lockout [2-131](#)  
   perform a lockout on a BLSR [2-130](#)  
   working span lockout [2-72](#)  
 LOCKOUT-REQ [2-72](#)  
 LOCKOUT-REQ-RING [2-72](#)  
 LOCKOUT-REQ-SPAN [2-72](#)  
 LOF  
   BITS [2-73](#)  
   DS-1 [2-74](#)  
   EC-1 [2-75](#)  
   OC-N [2-75](#)  
 LOF-DS3 [2-74](#)  
 log-in errors  
   applet security restrictions [1-53](#)  
   browser login does not launch Java [1-46](#)  
   browser stalls when downloading .jar file [1-50](#)  
   no DCC connection [1-57](#)  
   no IP connectivity [1-57](#)  
   username/password mismatch [1-56](#)  
 login node groups [3-2](#)  
 loopback  
   alarms [2-84, 2-85, 2-86, 2-87](#)  
   clear [2-132](#)  
   description [1-2](#)  
   perform a facility loopback [1-33](#)  
   see also facility loopback

see also terminal loopback

LOP-P [2-76](#)

LOP-V [2-77](#)

LOS

BITS [2-79](#)

DS-1 [2-79](#)

DS-3 [2-80](#)

EC-1 [2-81](#)

OC-N [2-82](#)

loss of frame see LOP

loss of pointer see LOP

loss of signal see FE-LOS

LPBKDS1FEAC [2-84](#)

LPBKDS1FEAC-CMD [2-84](#)

LPBKDS3FEAC [2-85](#)

LPBKDS3FEAC-CMD [2-85](#)

LPBKFACILITY

DS-N or EC-1 [2-85](#)

OC-N [2-86](#)

LPBKTERMINAL [2-87](#)

---

## M

MAC address

data memory failure [2-93](#)

invalid [2-71](#)

mismatch [1-61](#)

MAN-REQ [2-87](#)

MANRESET [2-88](#)

MANSWTOINT [2-88](#)

MANSWTOPRI [2-88](#)

MANSWTOSEC [2-88](#)

MANSWTO THIRD [2-89](#)

MANUAL-REQ-RING [2-89](#)

MANUAL-REQ-SPAN [2-89](#)

manual switch [1-10, 1-16](#)

manual switch see protection switching

MEA

backplane [2-89](#)

EQPT [2-90](#)

FAN [2-92](#)

MEM-GONE [2-93](#)

MEM-LOW [2-93](#)

MFGMEM [2-93](#)

---

## N

Netscape Navigator

clear cache [1-51](#)

log in [1-40, 3-2](#)

network testing

see hairpin circuits

see loopbacks

NIC card [1-47, 1-61](#)

node ID

change [2-129](#)

identify [2-129](#)

NOT-AUTHENTICATED (alarm) [1-56](#)

---

## O

OC-N cards

see also specific card names

bit errors [1-70](#)

lockout request condition [2-72](#)

LOF [2-75](#)

loopback caveat [1-2](#)

OC-192 temperature alarm [2-24](#)

OC-3 and DCC limitations [1-68](#)

replace [2-134](#)

reset [2-134](#)

test [1-30, 1-35](#)

transmit and receive levels [1-77](#)

---

## P

passwords

- login [3-2](#)
- password/ username mismatch [1-56](#)
- path trace [2-121](#)
- PDI-P [2-94](#)
- PEER-NORESPONSE [2-96](#)
- ping [1-48, 2-110](#)
- PLM-P [2-96](#)
- PLM-V [2-98](#)
- power
  - consumption [1-79](#)
  - isolate power supply problems [1-79](#)
  - low voltage battery alarm [2-43](#)
  - NE power failure (connector A) [2-100](#)
  - NE power failure (connector B) [2-100](#)
  - supply [1-78](#)
- PRC-DUPID [2-98](#)
- protection group
  - clear a switch [2-132](#)
  - delete [2-70](#)
  - perform a traffic switch [2-131](#)
- protection switching
  - UPSR alarms [2-27](#)
- PROTNA [2-99](#)
- PWR-A [2-100](#)
- PWR-B [2-100](#)

---

## R

- RAI [2-101](#)
- RCVR-MISS [2-101](#)
- receive levels [1-77](#)
- reset
  - automatic card-level reboot [2-25](#)
  - reseat the TCC+ standby [3-4](#)
- RFI
  - line level [2-102](#)
  - path level [2-102](#)
  - VT level [2-103](#)
- ring ID

- change [2-129](#)
- identify [2-129](#)
- RING-MISMATCH [2-104](#)
- RING-SW-EAST [2-104](#)
- RING-SW-WEST [2-104](#)

---

## S

- SD-L [2-105](#)
- SD-P [2-106](#)
- severities, alarm [2-14](#)
- SF-L [2-107](#)
- SF-P [2-108](#)
- side switch
  - initiate a side switch [2-131](#)
  - test standby cross-connect card [1-9](#)
- side switch see protection switching
- signal degrade [2-26](#)
- signal failure [2-26, 2-107, 2-108](#)
- SLMF [2-94](#)
- SMB connector [2-101, 2-123](#)
- SNTP [2-110](#)
- SNTP-HOST [2-110](#)
- SPAN-SW-EAST [2-110](#)
- SPAN-SW-WEST [2-111](#)
- SQUELCH [2-111](#)
- SSM
  - failure [2-113](#)
  - quality level degrade [2-112](#)
  - ST4 condition [2-115](#)
  - synchronization traceability alarm [2-115](#)
  - timing switch [1-68](#)
- SSM-DUS [2-112](#)
- SSM-FAIL [2-113](#)
- STS concatenation error [2-35](#)
- STSMON [2-25, 2-27](#)
- SWFTDWN [2-110](#)
- switching see automatic protection switching
- SWMTXMOD [2-116](#)

SWTOPRI [2-118](#)

SWTOSEC [2-118](#)

SWTOTHIRD [2-118](#)

SYNC-FREQ [2-118](#)

synchronization status messaging *see* SSM

SYNCPRI [2-119](#)

SYNCSEC [2-119](#)

SYNCTHIRD [2-120](#)

SYSBOOT [2-121](#)

## T

### TCC+ card

communication failure (TCC+ card to traffic card) [2-37](#),  
[2-38](#)

communication failure (TCC+ to TCC+) [2-36](#)

flash memory exceeded [2-42](#)

jar file download problem [1-50](#)

loss of signal from BITS [2-79](#)

low memory [2-93](#)

memory capacity exceeded [2-93](#)

reset [2-133](#)

### TCC2 card

communication failure (TCC2 card to traffic card) [2-37](#),  
[2-38](#)

communication failure (TCC2 to TCC2) [2-36](#)

TCP/IP [1-48](#), [2-28](#)

### Telcordia

default severities [2-1](#)

signal degrade definition [2-105](#), [2-106](#)

signal failure definition [2-107](#), [2-108](#)

trouble categories [2-14](#)

### temperature

fan-tray assembly alarm [2-55](#)

high-temperature alarm [2-67](#)

OC-192 alarm [2-24](#)

### terminal loopback

definition [1-2](#)

destination DS-N [1-11](#), [1-12](#)

destination OC-N [1-25](#), [1-36](#)

intermediate OC-N [1-31](#)

source OC-N [1-25](#)

### testing

*see* lamp test

*see* loopback

*see* power

### timing alarms

loss of primary reference [2-119](#)

loss of tertiary reference [2-120](#)

synchronization [2-66](#), [2-68](#)

timing reference failure [2-67](#)

### timing reference

automatic switch to secondary source (condition) [2-118](#)

automatic switch to third timing source  
(condition) [2-118](#)

change [2-70](#)

manual switch to internal source (condition) [2-88](#)

manual switch to primary source (condition) [2-88](#)

manual switch to second source (condition) [2-88](#)

manual switch to third source (condition) [2-89](#)

switch error [1-68](#)

TIM-P [2-121](#)

TL1 alarms [2-1](#)

topology hosts [3-2](#)

TPTFAIL [2-122](#)

transmission failure [2-123](#)

transmit levels [1-77](#)

TRMT [2-122](#)

TRMT-MISS [2-123](#)

troubleclearing *see* troubleshooting

troubleshooting [1-1 to 1-80](#)

*see also* alarm troubleshooting

*see also* loopback

conditions [2-14](#)

network tests [1-2](#)

severities [2-14](#)

trouble notifications [2-14](#)

---

**U**

## UNEQ

AUTOSW-UNEQ (STSMON) [2-27](#)

AUTOSW-UNEQ (VT-MON) [2-27](#)

UNEQ-P [2-124](#)

UNEQ-V [2-125](#)

## UPSR

AIS alarm [2-25](#)

clear a lockout [2-131](#)

failed switch path [2-51](#)

LOP alarm [2-25, 2-26](#)

PDI alarm [2-26](#)

SD alarm [2-26](#)

signal failure alarm [2-26](#)

username/password mismatch [1-56](#)

---

**V**

VirusScan [1-50](#)

voltage see battery

voltage see power

VT1.5 creation error [1-66](#)

VT-MON [2-27](#)

---

**W**

west/ east misconnection alarm [2-47](#)

WTR (condition) [1-40](#)

