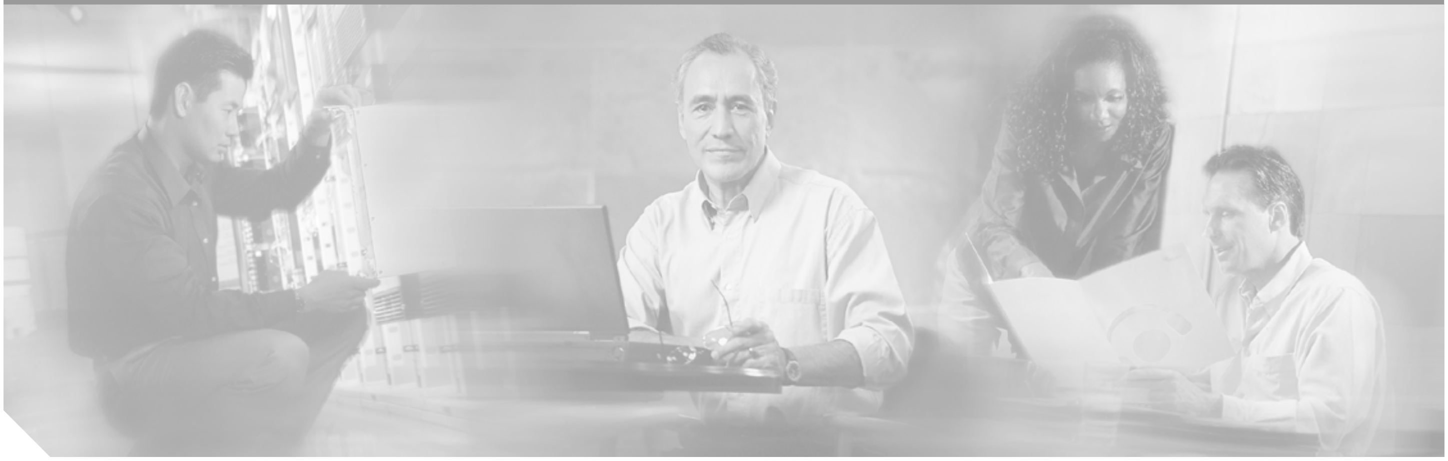


Cisco ONS 15454 Troubleshooting Guide

Product and Documentation Release 4.6
Last updated: August 21, 2007

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-7815982=
Text Part Number: 78-15982-02

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.

Cisco ONS 15454 Troubleshooting Guide

CONTENTS

About This Guide xxix

Revision History xxix

Document Objectives xxx

Audience xxx

Document Organization xxxi

Related Documentation xxxi

Document Conventions xxxi

Where to Find Safety and Warning Information xxxii

Obtaining Documentation xxxii

Cisco.com xxxii

Ordering Documentation xxxiii

Cisco Optical Networking Product Documentation CD-ROM xxxiii

Documentation Feedback xxxiii

Obtaining Technical Assistance xxxiii

Cisco Technical Support Website xxxiv

Submitting a Service Request xxxiv

Definitions of Service Request Severity xxxiv

Obtaining Additional Publications and Information xxxv

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 1-6

1.2.1 Perform a Facility (Line) Loopback on a Source DS-N Port 1-7

1.3 Identify Points of Failure on a DS-N Circuit Path 1-8

1.3.1 Perform a Facility (Line) Loopback on a Source DS-N Port (West to East) 1-8

Create the Facility (Line) Loopback on the Source DS-N Port 1-9

Test and Clear the Facility (Line) Loopback Circuit 1-9

Test the DS-N Cabling 1-10

Test the DS-N Card 1-10

Test the EIA 1-11

1.3.2 Perform a Hairpin Test on a Source Node Port (West to East) 1-12

Create the Hairpin Circuit on the Source Node Port 1-12

Test and Delete the Hairpin Circuit 1-13

Test the Standby XC10G Cross-Connect Card 1-13
Retest the Original XC10G Cross-Connect Card 1-14
1.3.3 Perform an XC Loopback on a Destination Node OC-N STS (West to East) 1-15
Test the XC Loopback Circuit 1-16
Test the Standby XC10G Cross-Connect Card 1-17
Retest the Original XC10G Cross-Connect Card 1-18
1.3.4 Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East) 1-18
Create the Terminal (Inward) Loopback on a Destination DS-N Port 1-19
Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port 1-20
Test the Destination DS-N Card 1-21
1.3.5 Perform a Facility (Line) Loopback on a Destination DS-N Port (East to West) 1-22
Create the Facility (Line) Loopback on the Destination DS-N Port 1-22
Test and Clear the Facility (Line) Loopback Circuit 1-23
Test the DS-N Cabling 1-23
Test the DS-N Card 1-24
Test the EIA 1-24
1.3.6 Perform a Hairpin Test on a Destination Node Port (East to West) 1-25
Create the Hairpin Circuit on the Destination Node Port 1-26
Test and Delete the Hairpin Circuit 1-26
Test the Standby XC10G Cross-Connect Card 1-27
Retest the Original XC10G Cross-Connect Card 1-28
1.3.7 Perform an XC Loopback on a Source Node OC-N STS (East to West) 1-29
Test the XC Loopback Circuit 1-30
Test the Standby XC10G Cross-Connect Card 1-30
Retest the Original XC10G Cross-Connect Card 1-31
1.3.8 Perform a Terminal (Inward) Loopback on a Source DS-N Port (East to West) 1-32
Create the Terminal (Inward) Loopback on a Source DS-N Port 1-33
Test and Clear the Terminal (Inward) Loopback Circuit on the Source DS-N Port 1-34
Test the Destination DS-N Card 1-34
1.4 Using the DS3XM-6 Card FEAC (Loopback) Functions 1-35
1.4.1 FEAC Send Code 1-36
1.4.2 DS-3I Inhibit Loopback 1-37
1.4.3 DS3XM-6 Inhibit FEAC Loopback 1-37
1.4.4 FEAC Alarms 1-37
1.5 Identify Points of Failure on an Optical Circuit Path 1-37
1.5.1 Perform a Facility (Line) Loopback on a Source-Node G-Series, MXP, OC-N, or TXP Port 1-38
Create the Facility (Line) Loopback on the Source Port 1-38
Test and Clear the Facility (Line) Loopback Circuit 1-39
Test the OC-N, G-Series, MXP, or TXP Card 1-39

1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port **1-40**

Create the Terminal (Inward) Loopback on a Source Node Port **1-41**

Test and Clear the Terminal Loopback Circuit **1-42**

Test the OC-N, G-Series, MXP, or TXP Card **1-43**

1.5.3 Create the XC Loopback on the Source OC-N Port **1-44**

Test the XC Loopback Circuit **1-45**

Test the Standby XC10G Cross-Connect Card **1-45**

Retest the Original XC10G Cross-Connect Card **1-46**

1.5.4 Create a Facility (Line) Loopback on an Intermediate-Node G-Series, MXP, OC-N, or TXP Port **1-47**

Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port **1-48**

Test and Clear the Facility (Line) Loopback Circuit **1-49**

Test the OC-N, G-Series, MXP, or TXP Card **1-50**

1.5.5 Create a Terminal (Inward) Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports **1-50**

Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports **1-51**

Test and Clear the Terminal Loopback Circuit **1-52**

Test the OC-N, G-Series, MXP, or TXP Card **1-53**

1.5.6 Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port **1-54**

Create the Facility (Line) Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port **1-54**

Test and Clear the Facility (Line) Loopback Circuit **1-55**

Test the OC-N, G-Series, MXP, or TXP Card **1-56**

1.5.7 Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port **1-57**

Create the Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port **1-57**

Test and Clear the Terminal Loopback Circuit **1-58**

Test the OC-N, G-Series, MXP, or TXP Card **1-59**

1.6 Restoring the Database and Default Settings **1-60**

1.6.1 Restore the Node Database **1-60**

Restore the Database **1-60**

1.6.2 Restore the Node to Factory Configuration **1-62**

Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) **1-63**

Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX) **1-64**

1.7 PC Connectivity Troubleshooting **1-66**

1.7.1 PC System Minimum Requirements **1-66**

1.7.2 Sun System Minimum Requirements **1-66**

1.7.3 Supported Platforms, Browsers, and JREs **1-66**

1.7.4 Unsupported Platforms and Browsers **1-67**

1.7.5 Unable to Verify the IP Configuration of Your PC 1-67

Verify the IP Configuration of Your PC 1-68

1.7.6 Browser Login Does Not Launch Java 1-68

Reconfigure the PC Operating System Java Plug-in Control Panel 1-68

Reconfigure the Browser 1-69

1.7.7 Unable to Verify the NIC Connection on Your PC 1-70

1.7.8 Verify PC Connection to the ONS 15454 (ping) 1-70

Ping the ONS 15454 1-71

1.7.9 The IP Address of the Node is Unknown 1-71

Retrieve Unknown Node IP Address 1-71

1.8 CTC Operation Troubleshooting 1-72

1.8.1 Unable to Launch CTC Help After Removing Netscape 1-72

Reset Internet Explorer as the Default Browser for CTC 1-72

1.8.2 Unable to Change Node View to Network View 1-73

Reset the CTC_HEAP Environment Variable for Windows 1-73

Reset the CTC_HEAP Environment Variable for Solaris 1-73

1.8.3 Browser Stalls When Downloading CTC JAR Files From TCC2 1-74

Disable the VirusScan Download Scan 1-74

1.8.4 CTC Does Not Launch 1-74

Redirect the Netscape Cache to a Valid Directory 1-75

1.8.5 Slow CTC Operation or Login Problems 1-75

Delete the CTC Cache File Automatically 1-75

Delete the CTC Cache File Manually 1-76

1.8.6 Node Icon is Gray on CTC Network View 1-77

1.8.7 CTC Cannot Launch Due to Applet Security Restrictions 1-77

Manually Edit the java.policy File 1-78

1.8.8 Java Runtime Environment Incompatible 1-78

Launch CTC to Correct the Core Version Build 1-79

1.8.9 Different CTC Releases Do Not Recognize Each Other 1-80

Launch CTC to Correct the Core Version Build 1-80

1.8.10 Username or Password Do Not Match 1-81

Verify Correct Username and Password 1-81

1.8.11 No IP Connectivity Exists Between Nodes 1-81

1.8.12 DCC Connection Lost 1-82

1.8.13 “Path in Use” Error When Creating a Circuit 1-82

1.8.14 Calculate and Design IP Subnets 1-83

1.8.15 Ethernet Connections 1-83

Verify Ethernet Connections 1-84

1.8.16 VLAN Cannot Connect to Network Device from Untag Port 1-85

Change VLAN Port Tag and Untagged Settings 1-85

1.8.17 Cross-Connect Card Oscillator Fails 1-86
1.8.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active 1-87
1.8.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active 1-87
1.9 Circuits and Timing 1-88
1.9.1 OC-N Circuit Transitions to Partial State 1-88
View the State of OC-N Circuit Nodes 1-89
1.9.2 AIS-V on DS3XM-6 Unused VT Circuits 1-89
Clear AIS-V on DS3XM-6 Unused VT Circuits 1-90
1.9.3 Circuit Creation Error with VT1.5 Circuit 1-90
1.9.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card 1-91
1.9.5 DS-3 Card Does Not Report AIS-P From External Equipment 1-91
1.9.6 OC-3 and DCC Limitations 1-92
1.9.7 ONS 15454 Switches Timing Reference 1-92
1.9.8 Holdover Synchronization Alarm 1-92
1.9.9 Free-Running Synchronization Mode 1-93
1.9.10 Daisy-Chained BITS Not Functioning 1-93
1.9.11 Blinking STAT LED after Installing a Card 1-93
1.10 Fiber and Cabling 1-94
1.10.1 Bit Errors Appear for a Traffic Card 1-94
1.10.2 Faulty Fiber-Optic Connections 1-95
Verify Fiber-Optic Connections 1-95
1.10.2.1 Crimp Replacement LAN Cables 1-97
1.10.2.2 Replace Faulty GBIC or SFP Connectors 1-98
Remove GBIC or SFP Connectors 1-100
Installing a GBIC with Clips 1-100
Installing a GBIC with a Handle 1-101
1.10.3 OC-N Card Transmit and Receive Levels 1-102
1.11 Power and LED Tests 1-102
1.11.1 Power Supply Problems 1-103
Isolate the Cause of Power Supply Problems 1-103
1.11.2 Power Consumption for Node and Cards 1-104
1.11.3 Lamp Tests for Card LEDs 1-104
Verify Card LED Operation 1-105
Verify G-Series Ethernet or FC_MR-4 Card LED Operation 1-105
Verify E-Series and ML-Series Ethernet Card LED Operation 1-106

CHAPTER 2 Alarm Troubleshooting 2-1
2.1 Alarm Index by Default Severity 2-1
2.1.1 Critical Alarms (CR) 2-2

2.1.2 Major Alarms (MJ) 2-2

2.1.3 Minor Alarms (MN) 2-3

2.1.4 NA Conditions 2-4

2.1.5 NR Conditions 2-5

2.2 Alarms and Conditions Indexed By Alphabetical Entry 2-6

2.3 Logical Object Type Definitions 2-9

2.4 Alarm Index by Logical Object Type 2-10

2.5 Trouble Notifications 2-19

2.5.1 Conditions 2-20

2.5.2 Severities 2-20

2.6 Safety Summary 2-20

2.7 Alarm Procedures 2-21

2.7.1 AIS 2-21

Clear the AIS Condition 2-22

2.7.2 AIS-L 2-22

Clear the AIS-L Condition 2-22

2.7.3 AIS-P 2-22

Clear the AIS-P Condition 2-23

2.7.4 AIS-V 2-23

Clear the AIS-V Condition 2-23

2.7.5 ALS 2-23

2.7.6 AMPLI-INIT 2-24

Clear the AMPLI-INIT Condition 2-24

2.7.7 APC-DISABLED 2-24

Clear the APC-DISABLED Alarm 2-24

2.7.8 APC-FAIL 2-25

Clear the APC-FAIL Alarm 2-25

2.7.9 APSB 2-26

Clear the APSB Alarm 2-26

2.7.10 APSC-IMP 2-27

Clear the APSC-IMP Alarm 2-27

2.7.11 APSCDFLTK 2-27

Clear the APSCDFLTK Alarm 2-28

2.7.12 APSC-IMP 2-28

Clear the APSC-IMP Alarm 2-29

2.7.13 APSCINCON 2-29

Clear the APSCINCON Alarm 2-29

2.7.14 APSCM 2-29

Clear the APSCM Alarm 2-30

2.7.15 APSCNMIS 2-30

Clear the APSCNMIS Alarm 2-30

2.7.16 APSIMP 2-31

Clear the APSIMP Condition 2-31

2.7.17 APSMM 2-32

Clear the APSMM Alarm 2-32

2.7.18 AS-CMD 2-32

Clear the AS-CMD Condition 2-32

2.7.19 AS-MT 2-33

Clear the AS-MT Condition 2-33

2.7.20 AUD-LOG-LOSS 2-34

Clear the AUD-LOG-LOSS Condition 2-34

2.7.21 AUD-LOG-LOW 2-34

2.7.22 AU-LOF 2-34

2.7.23 AUTOLSROFF 2-35

Clear the AUTOLSROFF Alarm 2-35

2.7.24 AUTORESET 2-36

Clear the AUTORESET Alarm 2-36

2.7.25 AUTOSW-AIS 2-36

Clear the AUTOSW-AIS Condition 2-37

2.7.26 AUTOSW-LOP (STSMON) 2-37

Clear the AUTOSW-LOP (STSMON) Condition 2-37

2.7.27 AUTOSW-LOP (VT-MON) 2-37

Clear the AUTOSW-LOP (VT-MON) Alarm 2-37

2.7.28 AUTOSW-PDI 2-38

Clear the AUTOSW-PDI Condition 2-38

2.7.29 AUTOSW-SDBER 2-38

Clear the AUTOSW-SDBER Condition 2-38

2.7.30 AUTOSW-SFBER 2-38

Clear the AUTOSW-SFBER Condition 2-39

2.7.31 AUTOSW-UNEQ (STSMON) 2-39

Clear the AUTOSW-UNEQ (STSMON) Condition 2-39

2.7.32 AUTOSW-UNEQ (VT-MON) 2-39

Clear the AUTOSW-UNEQ (VT-MON) Alarm 2-39

2.7.33 AWG-DEG 2-40

Clear the AWG-DEG Alarm 2-40

2.7.34 AWG-FAIL 2-40

Clear the AWG-FAIL Alarm 2-40

2.7.35 AWG-OVERTEMP 2-41

Clear the AWG-OVERTEMP Alarm 2-41

2.7.36 AWG-WARM-UP 2-41

2.7.37 BAT-FAIL 2-41

Clear the BAT-FAIL Alarm 2-42

2.7.38 BKUPMEMP 2-42

Clear the BKUPMEMP Alarm 2-42

2.7.39 BLSROSYNC 2-43

Clear the BLSROSYNC Alarm 2-43

2.7.40 CARLOSS (CLIENT) 2-43

Clear the CARLOSS (CLIENT) Alarm 2-43

2.7.41 CARLOSS (EQPT) 2-44

Clear the CARLOSS (EQPT) Alarm 2-44

2.7.42 CARLOSS (E100T, E1000F) 2-45

Clear the CARLOSS (E100T, E1000F) Alarm 2-45

2.7.43 CARLOSS (G1000) 2-46

Clear the CARLOSS (G1000) Alarm 2-47

2.7.44 CARLOSS (ML100T, ML1000) 2-49

Clear the CARLOSS (ML100T, ML1000) Alarm 2-49

2.7.45 CARLOSS (TRUNK) 2-50

Clear the CARLOSS (TRUNK) Alarm 2-50

2.7.46 CASETEMP-DEG 2-50

Clear the CASETEMP-DEG Alarm 2-50

2.7.47 CKTDOWN 2-51

Clear the CKTDOWN Alarm 2-51

2.7.48 CLDRESTART 2-53

Clear the CLDRESTART Condition 2-53

2.7.49 COMIOXC 2-54

Clear the COMIOXC Alarm 2-54

2.7.50 COMM-FAIL 2-54

Clear the COMM-FAIL Alarm 2-54

2.7.51 CONTBUS-A-18 2-55

Clear the CONTBUS-A-18 Alarm 2-55

2.7.52 CONTBUS-B-18 2-55

Clear the CONTBUS-B-18 Alarm 2-56

2.7.53 CONTBUS-IO-A 2-56

Clear the CONTBUS-IO-A Alarm 2-56

2.7.54 CONTBUS-IO-B 2-57

Clear the CONTBUS-IO-B Alarm 2-57

2.7.55 CTNEQPT-MISMATCH 2-58

Clear the CTNEQPT-MISMATCH Condition 2-59

2.7.56 CTNEQPT-PBPROT 2-59

Clear the CTNEQPT-PBPROT Alarm 2-60
2.7.57 CTNEQPT-PBWORK 2-61
Clear the CTNEQPT-PBWORK Alarm 2-61
2.7.58 DATAFLT 2-62
Clear the DATAFLT Alarm 2-62
2.7.59 DBOSYNC 2-62
Clear the DBOSYNC Alarm 2-63
2.7.60 DSP-COMM-FAIL 2-63
2.7.61 DSP-FAIL 2-63
Clear the DSP-FAIL Alarm 2-64
2.7.62 DS3-MISM 2-64
Clear the DS3-MISM Condition 2-64
2.7.63 DUP-IPADDR 2-65
Clear the DUP-IDADDR Alarm 2-65
2.7.64 DUP-NODENAME 2-65
Clear the DUP-NODENAME Alarm 2-65
2.7.65 EHIBATVG 2-66
Clear the EHIBATVG Alarm 2-66
2.7.66 ELWBATVG 2-66
Clear the ELWBATVG Alarm 2-66
2.7.67 EOC 2-66
Clear the EOC Alarm 2-67
2.7.68 EOC-L 2-68
Clear the EOC-L Alarm 2-69
2.7.69 EQPT 2-69
Clear the EQPT Alarm 2-70
2.7.70 EQPT-MISS 2-70
Clear the EQPT-MISS Alarm 2-70
2.7.71 ERFI-P-CONN 2-71
Clear the ERFI-P-CONN Condition 2-71
2.7.72 ERFI-P-PAYLD 2-71
Clear the ERFI-P-PAYLD Condition 2-71
2.7.73 ERFI-P-SRVR 2-71
Clear the ERFI-P-SRVR Condition 2-72
2.7.74 ERROR-CONFIG 2-72
Clear the ERROR-CONFIG Alarm 2-72
2.7.75 ETH-LINKLOSS 2-73
Clear the ETH-LINKLOSS Condition 2-73
2.7.76 E-W-MISMATCH 2-73
Clear the E-W-MISMATCH Alarm with a Physical Switch 2-74

Clear the E-W-MISMATCH Alarm in CTC 2-75

2.7.77 EXCCOL 2-75

Clear the EXCCOL Alarm 2-75

2.7.78 EXERCISE-RING-FAIL 2-76

Clear the EXERCISE-RING-FAIL Condition 2-76

2.7.79 EXERCISE-SPAN-FAIL 2-76

Clear the EXERCISE-SPAN-FAIL Condition 2-77

2.7.80 EXT 2-77

Clear the EXT Alarm 2-77

2.7.81 EXTRA-TRAF-PREEMPT 2-77

Clear the EXTRA-TRAF-PREEMPT Alarm 2-77

2.7.82 FAILTOSW 2-78

Clear the FAILTOSW Condition 2-78

2.7.83 FAILTOSW-PATH 2-79

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration 2-79

2.7.84 FAILTOSWR 2-79

Clear the FAILTOSWR Condition in a Four-Fiber BLSR Configuration 2-80

2.7.85 FAILTOSWS 2-81

Clear the FAILTOSWS Condition 2-81

2.7.86 FAN 2-83

Clear the FAN Alarm 2-83

2.7.87 FANDEGRADE 2-84

Clear the FANDEGRADE Alarm 2-84

2.7.88 FE-AIS 2-84

Clear the FE-AIS Condition 2-84

2.7.89 FEC-MISM 2-84

Clear the FEC-MISM Alarm 2-85

2.7.90 FE-DS1-MULTLOS 2-85

Clear the FE-DS1-MULTLOS Condition 2-85

2.7.91 FE-DS1-NSA 2-85

Clear the FE-DS1-NSA Condition 2-86

2.7.92 FE-DS1-SA 2-86

Clear the FE-DS1-SA Condition 2-86

2.7.93 FE-DS1-SNGLLOS 2-86

Clear the FE-DS1-SNGLLOS Condition 2-87

2.7.94 FE-DS3-NSA 2-87

Clear the FE-DS3-NSA Condition 2-87

2.7.95 FE-DS3-SA 2-88

Clear the FE-DS3-SA Condition 2-88

2.7.96 FE-EQPT-NSA 2-88

Clear the FE-EQPT-NSA Condition 2-88

2.7.97 FE-FRCDWKSWPR-RING 2-89

Clear the FE-FRCDWKSWPR-RING Condition 2-89

2.7.98 FE-FRCDWKSWPR-SPAN 2-89

Clear the FE-FRCDWKSWPR-SPAN Condition 2-90

2.7.99 FE-IDLE 2-90

Clear the FE-IDLE Condition 2-90

2.7.100 FE-LOCKOUTOFPR-SPAN 2-90

Clear the FE-LOCKOUTOFPR-SPAN Condition 2-91

2.7.101 FE-LOF 2-91

Clear the FE-LOF Condition 2-91

2.7.102 FE-LOS 2-91

Clear the FE-LOS Condition 2-92

2.7.103 FE-MANWKSWPR-RING 2-92

Clear the FE-MANWKSWPR-RING Condition 2-92

2.7.104 FE-MANWKSWPR-SPAN 2-92

Clear the FE-MANWKSWPR-SPAN Condition 2-93

2.7.105 FEPRLF 2-93

Clear the FEPRLF Alarm on a Four-Fiber BLSR 2-93

2.7.106 FIBERTEMP-DEG 2-94

Clear the FIBERTEMP-DEG Alarm 2-94

2.7.107 FORCED-REQ 2-94

Clear the FORCED-REQ Condition 2-94

2.7.108 FORCED-REQ-RING 2-94

Clear the FORCED-REQ-RING Condition 2-95

2.7.109 FORCED-REQ-SPAN 2-95

Clear the FORCED-REQ-SPAN Condition 2-95

2.7.110 FRCDSWTOINT 2-95

2.7.111 FRCDSWTOPRI 2-95

2.7.112 FRCDSWTOSEC 2-96

2.7.113 FRCDSWTOTHIRD 2-96

2.7.114 FRNGSYNC 2-96

Clear the FRNGSYNC Alarm 2-96

2.7.115 FSTSYNC 2-97

2.7.116 FULLPASSTHR-BI 2-97

Clear the FULLPASSTHR-BI Condition 2-97

2.7.117 GAIN-HDEG 2-97

Clear the GAIN-HDEG Alarm 2-97

2.7.118 GAIN-HFAIL 2-98

Clear the GAIN-HFAIL Alarm 2-98

2.7.119 GAIN-LDEG 2-98
Clear the GAIN-LDEG Alarm 2-99
2.7.120 GAIN-LFAIL 2-99
Clear the GAIN-LFAIL Alarm 2-99
2.7.121 GCC-EOC 2-100
Clear the GCC-EOC Alarm 2-100
2.7.122 GE-OOSYNC 2-100
Clear the GE-OOSYNC Alarm 2-100
2.7.123 HIBATVG 2-100
Clear the HIBATVG Alarm 2-101
2.7.124 HI-LASERBIAS 2-101
Clear the HI-LASERBIAS Alarm 2-101
2.7.125 HI-RXPOWER 2-102
Clear the HI-RXPOWER Alarm 2-102
2.7.126 HITEMP 2-103
Clear the HITEMP Alarm 2-103
2.7.127 HI-TXPOWER 2-103
Clear the HI-TXPOWER Alarm 2-104
2.7.128 HLDOVRSYNC 2-104
Clear the HLDOVRSYNC Alarm 2-104
2.7.129 I-HITEMP 2-105
Clear the I-HITEMP Alarm 2-105
2.7.130 IMPROPRMVL 2-105
Clear the IMPROPRMVL Alarm 2-106
2.7.131 INC-GFP-OUTOFFRAME 2-107
Clear the INC-GFP-OUTOFFRAME Condition 2-107
2.7.132 INC-GFP-SIGLOSS 2-108
Clear the INC-GFP-SIGLOSS Condition 2-108
2.7.133 INC-GFP-SYNCLOSS 2-108
Clear the INC-GFP-SYNCLOSS Condition 2-109
2.7.134 INC-ISD 2-109
2.7.135 INC-SIGLOSS 2-109
Clear the INC-SIGLOSS Alarm 2-109
2.7.136 INC-SYNCLOSS 2-110
Clear the INC-SYNCLOSS Alarm 2-110
2.7.137 INHSWPR 2-110
Clear the INHSWPR Condition 2-110
2.7.138 INHSWWKG 2-110
Clear the INHSWWKG Condition 2-111
2.7.139 INTRUSION-PSWD 2-111

Clear the INTRUSION-PSWD Condition 2-111

2.7.140 INVMACADR 2-111

Clear the INVMACADR Alarm 2-112

2.7.141 IOSCFGCOPY 2-113

2.7.142 KB-PASSTHR 2-114

Clear the KB-PASSTHR Condition 2-114

2.7.143 KBYTE-APS-CHANNEL-FAILURE 2-114

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm 2-114

2.7.144 LAN-POL-REV 2-114

Clear the LAN-POL-REV Condition 2-115

2.7.145 LASER-APR 2-115

2.7.146 LASERBIAS-DEG 2-115

Clear the LASERBIAS-DEG Alarm 2-115

2.7.147 LASERBIAS-FAIL 2-116

Clear the LASERBIAS-FAIL Alarm 2-116

2.7.148 LASEREOL 2-116

Clear the LASEREOL Alarm 2-117

2.7.149 LASERTEMP-DEG 2-117

Clear the LASERTEMP-DEG Alarm 2-117

2.7.150 LKOUTPR-S 2-118

Clear the LKOUTPR-S Condition 2-118

2.7.151 LKOUTWK-S (NA) 2-118

2.7.152 LMP-HELLODOWN 2-118

Clear the LMP-HELLODOWN Alarm 2-118

2.7.153 LMP-NDFAIL 2-118

Clear the LMP-NDFAIL Alarm 2-119

2.7.154 LOA 2-119

Clear the LOA Alarm 2-119

2.7.155 LOCKOUT-REQ 2-119

Clear the LOCKOUT-REQ Condition 2-120

2.7.156 LOF (BITS) 2-120

Clear the LOF (BITS) Alarm 2-120

2.7.157 LOF (CLIENT) 2-121

Clear the LOF (CLIENT) Alarm 2-121

2.7.158 LOF (DS1) 2-121

Clear the LOF (DS1) Alarm 2-121

2.7.159 LOF (DS3) 2-122

Clear the LOF (DS3) Alarm 2-122

2.7.160 LOF (EC1-12) 2-123

Clear the LOF (EC1-12) Alarm 2-123

2.7.161 LOF (OCN) 2-123
Clear the LOF (OCN) Alarm 2-124
2.7.162 LOF (TRUNK) 2-124
Clear the LOF (TRUNK) Alarm 2-124
2.7.163 LOM 2-124
Clear the LOM Alarm 2-124
2.7.164 LOP-P 2-125
Clear the LOP-P Alarm 2-125
2.7.165 LOP-V 2-125
Clear the LOP-V Alarm 2-126
2.7.166 LO-RXPOWER 2-126
Clear the LO-RXPOWER Alarm 2-126
2.7.167 LOS (BITS) 2-127
Clear the LOS (BITS) Alarm 2-127
2.7.168 LOS (CLIENT) 2-127
Clear the LOS (CLIENT) Alarm 2-128
2.7.169 LOS (DS1) 2-128
Clear the LOS (DS1) Alarm 2-128
2.7.170 LOS (DS3) 2-129
Clear the LOS (DS3) Alarm 2-130
2.7.171 LOS (EC1-12) 2-130
Clear the LOS (EC1-12) Alarm 2-130
2.7.172 LOS (FUDC) 2-131
Clear the LOS (FUDC) Alarm 2-131
2.7.173 LOS (MSUDC) 2-132
2.7.174 LOS (OCN) 2-132
Clear the LOS (OCN) Alarm 2-133
2.7.175 LOS (OTS) 2-134
Clear the LOS (OTS) Alarm 2-134
2.7.176 LOS (TRUNK) 2-135
Clear the LOS (TRUNK) Alarm 2-135
2.7.177 LOS-P 2-136
Clear the LOS-P Alarm 2-136
2.7.178 LO-TXPOWER 2-137
Clear the LO-TXPOWER Alarm 2-137
2.7.179 LPBKCRS 2-138
Clear the LPBKCRS Condition 2-138
2.7.180 LPBKDS1FEAC 2-139
Clear the LPBKDS1FEAC Condition 2-139
2.7.181 LPBKDS1FEAC-CMD 2-139

2.7.182 LPBKDS3FEAC 2-139

Clear the LPBKDS3FEAC Condition 2-140

2.7.183 LPBKDS3FEAC-CMD 2-140

2.7.184 LPBKFACILITY (CLIENT, TRUNK) 2-140

Clear the LPBKFACILITY (CLIENT, TRUNK) Condition 2-141

2.7.185 LPBKFACILITY (DS1, DS3) 2-141

Clear the LPBKFACILITY (DS1, DS3) Condition 2-141

2.7.186 LPBKFACILITY (EC1-12) 2-141

Clear the LPBKFACILITY (EC1-12) Condition 2-142

2.7.187 LPBKFACILITY (G1000) 2-142

Clear the LPBKFACILITY (G1000) Condition 2-142

2.7.188 LPBKFACILITY (OCN) 2-142

Clear the LPBKFACILITY (OCN) Condition 2-143

2.7.189 LPBKTERMINAL (CLIENT, TRUNK) 2-143

Clear the LPBKTERMINAL (CLIENT) Condition 2-143

2.7.190 LPBKTERMINAL (DS1, DS3, EC-1-12, OCN) 2-144

Clear the LPBKTERMINAL (DS1, DS3, EC1-12, OCN) Condition 2-144

2.7.191 LPBKTERMINAL (G1000) 2-144

Clear the LPBKTERMINAL (G1000) Condition 2-145

2.7.192 LWBATVG 2-145

Clear the LWBATVG Alarm 2-145

2.7.193 MAN-REQ 2-145

Clear the MAN-REQ Condition 2-145

2.7.194 MANRESET 2-146

2.7.195 MANSWTOINT 2-146

2.7.196 MANSWTOPRI 2-146

2.7.197 MANSWTOSEC 2-146

2.7.198 MANSWTOTHIRD 2-147

2.7.199 MANUAL-REQ-RING 2-147

Clear the MANUAL-REQ-RING Condition 2-147

2.7.200 MANUAL-REQ-SPAN 2-147

Clear the MANUAL-REQ-SPAN Condition 2-147

2.7.201 MEA (AIP) 2-148

Clear the MEA (AIP) Alarm 2-148

2.7.202 MEA (EQPT) 2-148

Clear the MEA (EQPT) Alarm 2-148

2.7.203 MEA (FAN) 2-150

Clear the MEA (FAN) Alarm 2-150

2.7.204 MEM-GONE 2-151

2.7.205 MEM-LOW 2-151

2.7.206 MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN) 2-151

Clear the MFGMEM (AICI-AEP, AIE, BPLANE, FAN) Alarm 2-152

2.7.207 NO-CONFIG 2-152

Clear the NO-CONFIG Condition 2-152

2.7.208 NOT-AUTHENTICATED 2-153

2.7.209 NTWTPINC 2-153

2.7.210 OCHNC-ACTIV-FAIL 2-153

2.7.211 OCHNC-DEACTIV-FAIL 2-153

2.7.212 OCHNC-FAIL 2-153

2.7.213 OCHNC-INC 2-153

2.7.214 ODUK-AIS-PM 2-154

Clear the ODUK-AIS-PM Condition 2-154

2.7.215 ODUK-BDI-PM 2-154

Clear the ODUK-BDI-PM Condition 2-154

2.7.216 ODUK-LCK-PM 2-155

Clear the ODUK-LCK-PM Condition 2-155

2.7.217 ODUK-OCI-PM 2-155

Clear the ODUK-OCI-PM Condition 2-155

2.7.218 ODUK-SD-PM 2-156

Clear the ODUK-SD-PM Condition 2-156

2.7.219 ODUK-SF-PM 2-156

Clear the ODUK-SF-PM Condition 2-156

2.7.220 ODUK-TIM-PM 2-156

Clear the ODUK-TIM-PM Condition 2-157

2.7.221 OOU-TPT 2-157

Clear the OOT-TPT Condition 2-157

2.7.222 OPTNTWMIS 2-157

Clear the OPTNTWMIS Alarm 2-158

2.7.223 OPWR-HDEG 2-158

Clear the OPWR-HDEG Alarm 2-158

2.7.224 OPWR-HFAIL 2-160

Clear the OPWR-HFAIL Alarm 2-160

2.7.225 OPWR-LDEG 2-160

Clear the OPWR-LDEG Alarm 2-160

2.7.226 OPWR-LFAIL 2-161

Clear the OPWR-LFAIL Alarm 2-161

2.7.227 OTUK-AIS 2-161

Clear the OTUK-AIS Condition 2-161

2.7.228 OTUK-BDI 2-162

Clear the OTUK-BDI Condition 2-162

2.7.229 OTUK-LOF 2-162

Clear the OTUK-LOF Alarm 2-162

2.7.230 OTUK-SD 2-163

Clear the OTUK-SD Condition 2-163

2.7.231 OTUK-SF 2-163

Clear the OTUK-SF Condition 2-163

2.7.232 OTUK-TIM 2-164

Clear the OTUK-TIM Condition 2-164

2.7.233 OUT-OF-SYNC 2-164

Clear the OUT-OF-SYNC Condition 2-164

2.7.234 PDI-P 2-164

Clear the PDI-P Condition 2-165

2.7.235 PEER-NORESPONSE 2-166

Clear the PEER-NORESPONSE Alarm 2-166

2.7.236 PLM-P 2-167

Clear the PLM-P Alarm 2-167

2.7.237 PLM-V 2-167

Clear the PLM-V Alarm 2-168

2.7.238 PORT-CODE-MISM 2-168

Clear the PORT-CODE-MISM Alarm 2-168

2.7.239 PORT-COMM-FAIL 2-168

Clear the PORT-COMM-FAIL Alarm 2-169

2.7.240 PORT-MISMATCH 2-169

2.7.241 PORT-MISSING 2-169

Clear the PORT-MISSING Alarm 2-169

2.7.242 PRC-DUPID 2-170

Clear the PRC-DUPID Alarm 2-170

2.7.243 PROTNA 2-170

Clear the PROTNA Alarm 2-170

2.7.244 PTIM 2-171

Clear the PTIM Alarm 2-171

2.7.245 PWR-A 2-171

2.7.246 PWR-B 2-171

2.7.247 PWR-REDUN 2-172

Clear the PWR-REDUN Alarm 2-172

2.7.248 RAI 2-172

Clear the RAI Condition 2-172

2.7.249 RCVR-MISS 2-173

Clear the RCVR-MISS Alarm 2-173

2.7.250 RFI 2-173

Clear the RFI Condition 2-173

2.7.251 RFI-L 2-174

Clear the RFI-L Condition 2-174

2.7.252 RFI-P 2-174

Clear the RFI-P Condition 2-174

2.7.253 RFI-V 2-175

Clear the RFI-V Condition 2-175

2.7.254 RING-ID-MIS 2-176

Clear the RING-ID-MIS Alarm 2-176

2.7.255 RING-MISMATCH 2-176

Clear the RING-MISMATCH Alarm 2-176

2.7.256 RING-SW-EAST 2-177

2.7.257 RING-SW-WEST 2-177

2.7.258 RSVP-HELLODOWN 2-177

Clear the RSVP-HELLODOWN Alarm 2-177

2.7.259 RUNCFG-SAVENEED 2-178

2.7.260 SD (CLIENT, TRUNK) 2-178

Clear the SD (CLIENT or TRUNK) Condition 2-178

2.7.261 SD (DS1, DS3) 2-178

Clear the SD (DS1, DS3) Condition 2-179

2.7.262 SD-L 2-180

Clear the SD-L Condition 2-180

2.7.263 SD-P 2-180

Clear the SD-P Condition 2-181

2.7.264 SF (CLIENT, TRUNK) 2-181

Clear the SF (CLIENT, TRUNK) Condition 2-181

2.7.265 SF (DS1, DS3) 2-182

Clear the SF (DS1, DS3) Condition 2-182

2.7.266 SF-L 2-182

Clear the SF-L Condition 2-182

2.7.267 SF-P 2-183

Clear the SF-P Condition 2-183

2.7.268 SFTWDOWN 2-183

2.7.269 SH-INS-LOSS-VAR-DEG-HIGH 2-183

2.7.269.1 Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm 2-184

2.7.270 SH-INS-LOSS-VAR-DEG-LOW 2-184

2.7.270.1 Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm 2-184

2.7.271 SHUTTER-OPEN 2-184

Clear the SHUTTER-OPEN Alarm 2-184

2.7.272 SNTP-HOST 2-185

Clear the SNTP-HOST Alarm 2-185

2.7.273 SPAN-SW-EAST 2-185

2.7.274 SPAN-SW-WEST 2-186

2.7.275 SQUELCH 2-186

Clear the SQUELCH Condition 2-186

2.7.276 SQUELCHED 2-187

Clear the SQUELCHED Alarm 2-187

2.7.277 SQM 2-188

Clear the SQM Alarm 2-188

2.7.278 SSM-DUS 2-188

2.7.279 SSM-FAIL 2-189

Clear the SSM-FAIL Alarm 2-189

2.7.280 SSM-LNC 2-189

2.7.281 SSM-OFF 2-189

Clear the SSM-OFF Condition 2-190

2.7.282 SSM-PRC 2-190

2.7.283 SSM-PRS 2-190

2.7.284 SSM-RES 2-190

2.7.285 SSM-SDH-TN 2-190

2.7.286 SSM-SETS 2-191

2.7.287 SSM-SMC 2-191

2.7.288 SSM-STU 2-191

Clear the SSM-STU Condition 2-191

2.7.289 SSM-ST2 2-191

2.7.290 SSM-ST3 2-192

2.7.291 SSM-ST3E 2-192

2.7.292 SSM-ST4 2-192

2.7.293 SSM-TNC 2-192

2.7.294 SWMTXMOD 2-193

Clear the SWMTXMOD Alarm 2-193

2.7.295 SWTOPRI 2-194

2.7.296 SWTOSEC 2-194

Clear the SWTOSEC Condition 2-194

2.7.297 SWTOTHIRD 2-194

Clear the SWTOTHIRD Condition 2-195

2.7.298 SYNC-FREQ 2-195

Clear the SYNC-FREQ Condition 2-195

2.7.299 SYNCPRI 2-195

Clear the SYNCPRI Alarm 2-196

2.7.300 SYNCSEC 2-196

Clear the SYNCSEC Alarm 2-196
2.7.301 SYNCTHIRD 2-197
Clear the SYNCTHIRD Alarm 2-197
2.7.302 SYSBOOT 2-197
2.7.303 TIM 2-198
Clear the TIM Alarm or Condition 2-198
2.7.304 TIM-MON 2-198
Clear the TIM-MON Alarm 2-199
2.7.305 TIM-P 2-199
Clear the TIM-P Alarm 2-199
2.7.306 TPTFAIL (FC_MR-4) 2-200
Clear the TPTFAIL (FC_MR-4) Alarm 2-200
2.7.307 TPTFAIL (G1000) 2-200
Clear the TPTFAIL (G1000) Alarm 2-200
2.7.308 TPTFAIL (ML100T, ML1000) 2-201
Clear the TPTFAIL (ML100T, ML1000) Alarm 2-201
2.7.309 TRMT 2-201
Clear the TRMT Alarm 2-202
2.7.310 TRMT-MISS 2-202
Clear the TRMT-MISS Alarm 2-202
2.7.311 TX-AIS 2-203
Clear the TX-AIS Condition 2-203
2.7.312 TX-RAI 2-203
Clear the TX-RAI Condition 2-203
2.7.313 UNC-WORD 2-203
Clear the UNC-WORD Condition 2-203
2.7.314 UNEQ-P 2-204
Clear the UNEQ-P Alarm 2-204
2.7.315 UNEQ-V 2-206
Clear the UNEQ-V Alarm 2-206
2.7.316 VCG-DEG 2-206
Clear the VCG-DEG Condition 2-207
2.7.317 VCG-DOWN 2-207
Clear the VCG-DOWN Condition 2-207
2.7.318 VOA-HDEG 2-207
Clear the VOA-HDEG Alarm 2-207
2.7.319 VOA-HFAIL 2-208
Clear the VOA-HFAIL Alarm 2-208
2.7.320 VOA-LDEG 2-208
Clear the VOA-LDEG Alarm 2-209

2.7.321 VOA-LFAIL 2-209

Clear the VOA-LFAIL Alarm 2-209

2.7.322 WKSWPR 2-209

Clear the WKSWPR Condition 2-210

2.7.323 WTR 2-210

2.7.324 WVL-MISMATCH 2-210

Clear the WVL-MISMATCH alarm 2-210

2.8 DS3-12 E Line Alarms 2-211

2.9 DWDM and Non-DWDM Card LED Activity 2-212

2.9.1 DWDM Card LED Activity After Insertion 2-212

2.9.2 Non-DWDM Card LED Activity After Insertion 2-212

2.9.3 DWDM Card LED Activity During Reset 2-212

2.9.4 Non-DWDM Card LED Activity During Reset 2-212

2.9.5 Non-DWDM Cross-Connect LED Activity During Side Switch 2-213

2.9.6 Non-DWDM Card LED State After Successful Reset 2-213

2.10 Common Procedures in Alarm Troubleshooting 2-213

Identify a BLSR Ring Name or Node ID Number 2-213

Change a BLSR Ring Name 2-213

Change a BLSR Node ID Number 2-214

Verify Node Visibility for Other Nodes 2-214

Verify or Create Node DCC Terminations 2-214

Lock Out a BLSR Span 2-215

Clear a BLSR External Switching Command 2-215

Clear a Path Protection Lockout 2-215

Switch Protection Group Traffic with an External Switching Command 2-216

Side Switch the Active and Standby XC10G Cross-Connect cards 2-216

Clear a Protection Group External Switching Command 2-216

Delete a Circuit 2-217

Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback 2-217

Reset Active TCC2 Card and Activate Standby Card 2-217

Remove and Reinsert (Reseat) the Standby TCC2 2-218

Reset a Traffic Card in CTC 2-218

Verify BER Threshold Level 2-219

Physically Replace a Card 2-219

Remove and Reinsert (Reseat) a Card 2-219

Remove and Reinsert Fan-Tray Assembly 2-220

CHAPTER 3 Replace Hardware 3-1

3.1 Replace an In-Service Cross-Connect Card 3-2

3.2 Replace the Air Filter 3-5

3.2.1 Inspect, Clean, and Replace the Reusable Air Filter 3-5

3.2.2 Inspect and Replace the Disposable Air Filter 3-7

3.3 Determine Fan-Tray and AIP Replacement Compatibility 3-9

3.4 Replace the Fan-Tray Assembly 3-10

3.5 Replace the Alarm Interface Panel 3-12

3.6 Replace an Electrical Interface Assembly 3-17

3.7 Replace the Gigabit Interface Converter 3-18

3.8 Replace the Small Form-Factor Pluggable Connector 3-19

3.9 Install the Plastic Lower Backplane Cover 3-19

CHAPTER 4 Error Messages 4-1

INDEX

FIGURES

Figure 1-1 Facility (Line) Loopback Process on a DS-N Card 1-2

Figure 1-2 Facility (Line) Loopback Process on an OC-N Card 1-3

Figure 1-3 Terminal Loopback Process on an OC-N Card 1-3

Figure 1-4 Terminal Loopback Process on a DS-N Card 1-4

Figure 1-5 Terminal Loopback on a DS-N Card with Bridged Signal 1-5

Figure 1-6 Terminal Loopback on an OC-N Card with Bridged Signal 1-5

Figure 1-7 Hairpin Circuit Process on a DS-N Card 1-6

Figure 1-8 A Facility (Line) Loopback on a Circuit Source DS-N Port 1-7

Figure 1-9 Hairpin Circuit Process on a DS-N Card 1-7

Figure 1-10 A Facility (Line) Loopback on a Circuit Source DS-N Port 1-8

Figure 1-11 Hairpin on a Source Node Port 1-12

Figure 1-12 XC Loopback on a Destination OC-N Port 1-15

Figure 1-13 Terminal (Inward) Loopback on a Destination DS-N Port 1-19

Figure 1-14 A Facility (Line) Loopback on a Circuit Destination DS-N Port 1-22

Figure 1-15 Hairpin on a Destination Node Port 1-25

Figure 1-16 XC Loopback on a Source OC-N Port 1-29

Figure 1-17 Terminal (Inward) Loopback on a Source DS-N Port 1-32

Figure 1-18 Accessing FEAC Functions on the DS3XM-6 Card 1-36

Figure 1-19 Diagram of FEAC 1-36

Figure 1-20 Facility (Line) Loopback on a Circuit Source OC-N Port 1-38

Figure 1-21 Terminal (Inward) Loopback on a Source-Node OC-N Port 1-40

Figure 1-22 Terminal (Inward) Loopback on a G-Series Port 1-41

Figure 1-23 XC Loopback on a Source OC-N Port 1-44

Figure 1-24 Facility (Line) Loopback on an Intermediate-Node OC-N Port 1-47

Figure 1-25 Terminal Loopback on an Intermediate-Node OC-N Port 1-51

Figure 1-26 Facility (Line) Loopback on a Destination Node OC-N Port 1-54

Figure 1-27 Terminal Loopback on a Destination Node OC-N Port 1-57

Figure 1-28 Reinitialization Tool in Windows 1-63

Figure 1-29 Reinitialization Tool in UNIX 1-65

Figure 1-30 Deleting the CTC Cache 1-76

Figure 1-31 Ethernet Connectivity Reference 1-83

Figure 1-32 VLAN with Ethernet Ports at Tagged and Untag 1-85
Figure 1-33 Configuring VLAN Membership for Individual Ethernet Ports 1-86
Figure 1-34 RJ-45 Pin Numbers 1-97
Figure 1-35 LAN Cable Layout 1-97
Figure 1-36 Cross-Over Cable Layout 1-98
Figure 1-37 GBICs 1-99
Figure 1-38 GBIC Installation (with Clips) 1-101
Figure 2-1 Shelf LCD Panel 2-35
Figure 3-1 Reusable Fan-Tray Air Filter in an External Filter Bracket (Front Door Removed) 3-6
Figure 3-2 Inserting or Removing the Fan-Tray Assembly (Front Door Removed) 3-8
Figure 3-3 Inserting or Removing a Disposable Fan-Tray Air Filter (Front Door Removed) 3-8
Figure 3-4 Removing or Replacing the Fan-Tray Assembly (Front Door Removed) 3-12
Figure 3-5 Find the MAC Address 3-14
Figure 3-6 Lower Backplane Cover 3-14
Figure 3-7 Repairing Circuits 3-16
Figure 3-8 Recording the Old MAC Address Before Replacing the AIP 3-16
Figure 3-9 Circuit Repair Information 3-17
Figure 3-10 Attaching Plastic Lower Backplane Cover 3-20
Figure 4-1 Error Dialog Box 4-1

TABLES

Table 1-1 DS-N, OC-N, EC-N, and TXP/MXP Card Loopback Behavior 1-4

Table 1-2 Restore the Node Database 1-60

Table 1-3 Restore the Node to Factory Configuration 1-62

Table 1-4 Unable to Verify the IP Configuration of Your PC 1-67

Table 1-5 Browser Login Does Not Launch Java 1-68

Table 1-6 Unable to Verify the NIC Connection on your PC 1-70

Table 1-7 Verify PC Connection to ONS 15454 (ping) 1-70

Table 1-8 Retrieve the Unknown IP Address of the Node 1-71

Table 1-9 Unable to Launch CTC Help After Removing Netscape 1-72

Table 1-10 Browser Stalls When Downloading Files From TCC2 1-73

Table 1-11 Browser Stalls When Downloading JAR Files from TCC2 1-74

Table 1-12 CTC Does Not Launch 1-75

Table 1-13 Slow CTC Operation or Login Problems 1-75

Table 1-14 Node Icon is Gray on CTC Network View 1-77

Table 1-15 CTC Cannot Launch Due to Applet Security Restrictions 1-78

Table 1-16 Java Runtime Environment Incompatible 1-79

Table 1-17 JRE Compatibility 1-79

Table 1-18 Different CTC Releases Do Not Recognize Each Other 1-80

Table 1-19 Username or Password Do Not Match 1-81

Table 1-20 No IP Connectivity Exists Between Nodes 1-81

Table 1-21 DCC Connection Lost 1-82

Table 1-22 “Path in Use” Error When Creating a Circuit 1-82

Table 1-23 Calculate and Design IP Subnets 1-83

Table 1-24 Calculate and Design IP Subnets 1-83

Table 1-25 Verify VLAN Connection to Network Device from Untag Port 1-85

Table 1-26 Cross-Connect Card Oscillator Fails 1-87

Table 1-27 Circuit in Partial State 1-89

Table 1-28 Calculate and Design IP Subnets 1-90

Table 1-29 Circuit Creation Error with VT1.5 Circuit 1-91

Table 1-30 Unable to Create Circuit from DS-3 Card to DS3XM-6 Card 1-91

Table 1-31 DS3 Card Does Not Report AIS-P From External Equipment 1-91

Table 1-32 OC-3 and DCC Limitations 1-92
Table 1-33 ONS 15454 Switches Timing Reference 1-92
Table 1-34 Holdover Synchronization Alarm 1-93
Table 1-35 Free-Running Synchronization Mode 1-93
Table 1-36 Daisy-Chained BITS Sources Not Functioning 1-93
Table 1-37 Blinking STAT LED on Installed Card 1-94
Table 1-38 Bit Errors Appear for a Line Card 1-94
Table 1-39 Faulty Fiber-Optic Connections 1-95
Table 1-40 LAN Cable Pinout 1-98
Table 1-41 Cross-Over Cable Pinout 1-98
Table 1-42 Available GBICs 1-99
Table 1-43 Available SFPs 1-100
Table 1-44 OC-N Card Transmit and Receive Levels 1-102
Table 1-45 Power Supply Problems 1-103
Table 1-46 Power Consumption for Node and Cards 1-104
Table 1-47 Lamp Test for Optical and Electrical Card LEDs 1-105
Table 1-48 Lamp Test for G-Series or FC_MR-4 Card LEDs 1-105
Table 1-49 Lamp Test for E-Series and ML-Series Ethernet Card LEDs 1-106
Table 2-1 Critical Alarm Index 2-2
Table 2-2 Major Alarm Index 2-2
Table 2-3 Minor Alarm Index 2-3
Table 2-4 NA Conditions Index 2-4
Table 2-5 NR Conditions Index 2-5
Table 2-6 Alphabetical Alarm Index 2-6
Table 2-7 Alarm Type/Object Definition 2-9
Table 2-8 Alarm Index by Alarm Type 2-11
Table 2-9 DS3-12E Line Alarms 2-211
Table 3-1 Incompatibility Alarms 3-9
Table 4-1 Error Messages 4-1

About This Guide

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

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

Revision History

Date	Notes
03/30/2007	Revision History Table added for the first time
08/21/2007	Updated About this Guide

This section provides the following information:

- Document Objectives
- Audience
- Document Organization
- Related Documentation
- Document Conventions
- Where to Find Safety and Warning Information
- Obtaining Documentation
- Documentation Feedback
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

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

Audience

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

Document Organization

This Cisco ONS 15454 Troubleshooting Guide, R4.6 is organized into the following chapters:

- Chapter 1, "General Troubleshooting," provides methods to discover hardware errors, such as failed ports, that adversely affect signal traffic; it also gives typical software problems that occur and their solutions.
- Chapter 2, "Alarm Troubleshooting," provides indexes, descriptions, and troubleshooting methods for all alarms and conditions generated by the ONS system.
- Chapter 3, "Replace Hardware," provides methods for replacing failed hardware.
- Chapter 4, "Error Messages," provides a comprehensive list of all ONS system error messages and their identification numbers.

Related Documentation

Use this Cisco ONS 15454 Troubleshooting Guide, R4.6 in conjunction with the following referenced publications:

- *Cisco ONS 15454 Procedure Guide*
  Provides procedures (NTPs and DLPs) to install and configure the system.
- *Cisco ONS 15454 Reference Manual*
  Provides relevant information such as specifications or system use information.

Refer to the following standards documentation referenced in this publication:

- Telcordia GR-253 CORE

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.

Convention	Application
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15454 product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

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 (1 800 553-2447).

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

This chapter 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 Procedure Guide*.

- Identify Points of Failure on a DS-N Circuit Path—Explains how to perform the tests described in the "1.1 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 Optical Circuit Path—Explains how to perform the tests described in the "1.1 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 login 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.
- Power and LED Tests—Provides troubleshooting procedures for power supply and LED indicator problems.

1.1 Network Troubleshooting Tests

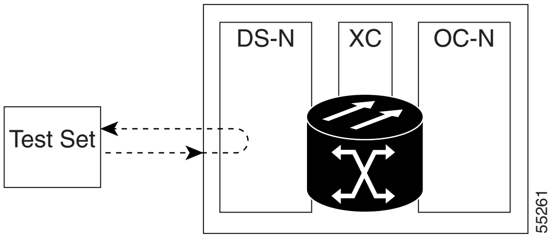
Use loopbacks and hairpin circuits to test newly created SONET circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 OC-N cards, transponder cards (TXP, TXPP), muxponder (MXP) cards, and G-Series Ethernet cards allow loopbacks and hairpin test circuits. Other cards do not allow loopbacks. These include ONS E-Series Ethernet, ML-Series Ethernet, and DWDM cards such as OPT-BST, OPT-PRE, OSC-CSM, band add-drop cards, and channel add-drop cards.

Caution Facility (line) or terminal loopbacks can be service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For more information about these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

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

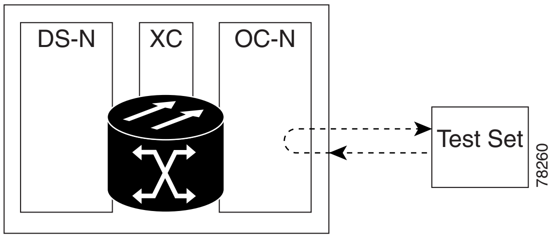
A facility (line) loopback tests the line interface unit (LIU) of a card, the EIA (electrical interface assembly), and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or the cabling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

Figure 1-1 Facility (Line) 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 (line) loopback or use a loopback or hairpin circuit on a card that is farther along the circuit path. Figure 1-2 shows a facility loopback on an OC-N card.

Figure 1-2 Facility (Line) Loopback Process on an OC-N Card



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

A terminal loopback tests a circuit path as it passes through the cross-connect card (XC10G) and loops back from the card with the loopback. Figure 1-3 shows a terminal loopback on an OC-N card. (Ethernet, transponder, and muxponder loopbacks follow the same model.) The test-set traffic comes into 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.

Setting a terminal loopback on the G-Series card might not stop the Tx Packets counter or the Rx Packet counters on the CTC card-level view Performance > Statistics page from increasing. The counters can increment even though the loopbacked port has temporarily disabled the transmit laser and is dropping any received packets.

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

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

Figure 1-3 Terminal Loopback Process on an OC-N Card

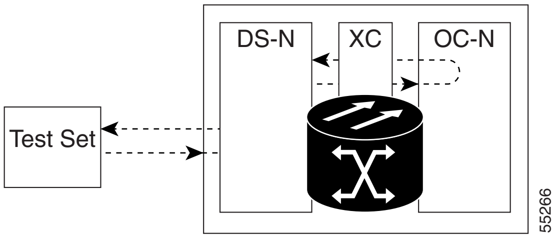
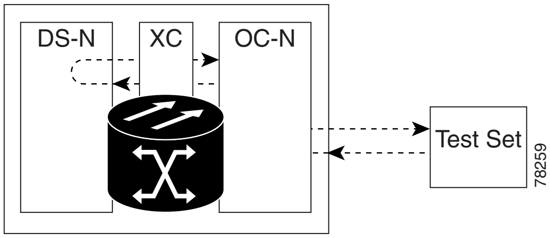


Figure 1-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the 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 Terminal Loopback Process on a DS-N Card



ONS 15454 port loopbacks either terminate or bridge the loopback signal. In the ONS 15454 system, all optical, electrical, Ethernet, and TXP/MXP facility loopbacks are terminated as shown in Table 1-1. During terminal loopbacks, some ONS cards bridge the loopback signal while others terminate it.

If an optical, electrical, Ethernet, and TXP/MXP port terminates a terminal or facility loopback signal, this means that the signal only loops back to the originating port and is not transmitted downstream. If the port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.

All ONS 15454 card bridging and terminating behaviors are listed in Table 1-1. When a port on a card in the left column of this table originates a terminal or facility loopback, the signal behaves as listed in the middle and right columns.

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

Table 1-1 DS-N, OC-N, EC-N, and TXP/MXP Card Loopback Behavior

Card/Port	Terminal loopback signal	Facility loopback signal
DS-1	Terminated	Terminated
DS-3	Bridged	Terminated
DS-N transmux	Bridged	Terminated
All OC-N cards	Bridged	Terminated
EC-1	Bridged	Terminated
G-Series Ethernet	Terminated[1]	Terminated[2]
TXP_MR_2.5G	Bridged	Terminated
TXP_MR_10G	Bridged	Terminated[3]
MXP_2.5G_10G	Bridged	Terminated[4]

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

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

3. A facility loopback on the client or trunk squelches the far end.
4. A facility loopback when the card is in transparent mode on the client or trunk squelches the far end.

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

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

- If a DS-N, OC-N, or EC-1 port is placed in out of service (OOS) state, it injects an AIS signal upstream and downstream.
- If a DS-N, OC-N, or EC-1 port is placed in out of service auto in-service (OOS_AINS) state or in the out of service maintenance (OOS_MT) state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected. For more information about placing ports into alternate states for testing, refer to the *Cisco ONS 15454 Procedure Guide*.
- If a TXP_MR_2.5G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises an Alarms Suppressed for Maintenance (AS-MT) condition during the loopback on the client side port.
- If a TXP_MR_10G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises a Loss of Signal (LOS) alarm on the DWDM-side port during the loopback.
- If an MXP_2.5_10G port is placed in the out of service maintenance (OOS_MT) state before loopback testing, the port raises a Loss of Signal (LOS) alarm on the DWDM-side port during the loopback.

Bridged DS-N and OC-N terminal loopback examples are shown in Figure 1-5 and Figure 1-6.

Figure 1-5 Terminal Loopback on a DS-N Card with Bridged Signal

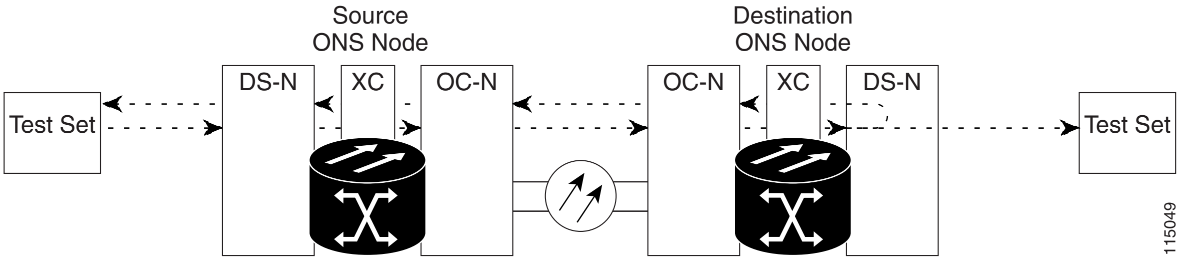
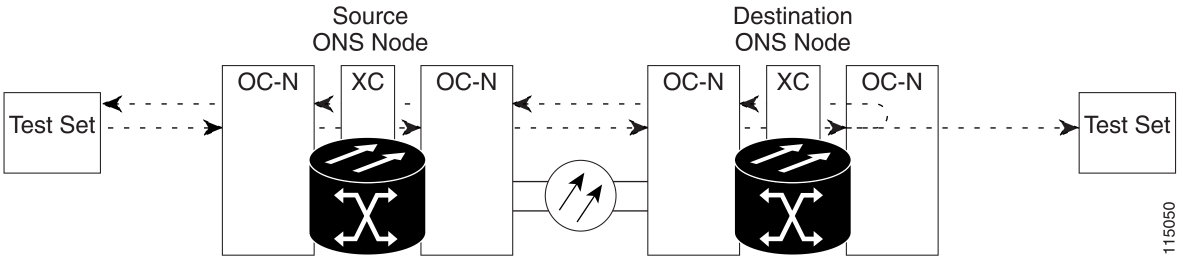
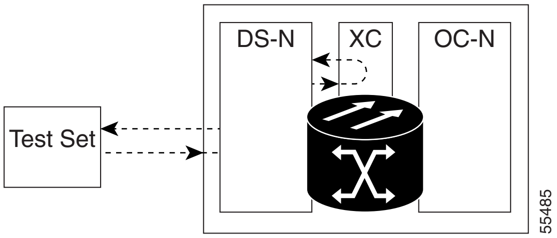


Figure 1-6 Terminal Loopback on an OC-N Card with Bridged Signal



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 1-9 shows the hairpin circuit process on a DS-N card.

Figure 1-7 Hairpin Circuit Process on a DS-N Card



A cross-connect loopback tests a circuit path as it passes through the cross-connect card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel at supported payloads at the STS-1 granularity and higher. For example, you can loop back a single STS-1, STS-3c, STS-6c, etc. on an optical facility (line) without interrupting the other STS circuits.

The following restrictions apply to cross-connect loopbacks:

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

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

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

The example in this section tests 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 sample scenario:

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

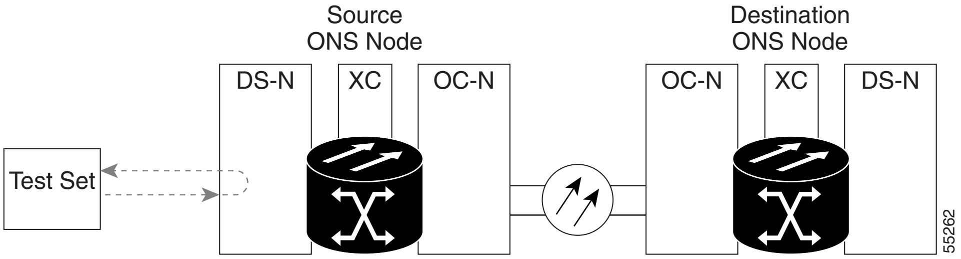
1. A facility (line) loopback on the source node DS-N
2. A hairpin on the source node DS-N
3. A terminal (inward) loopback on the destination node DS-N
4. A hairpin on the destination node DS-N
5. A facility (line) loopback on the destination DS-N

Note All loopback tests require on-site personnel.

1.2.1 Perform a Facility (Line) Loopback on a Source DS-N Port

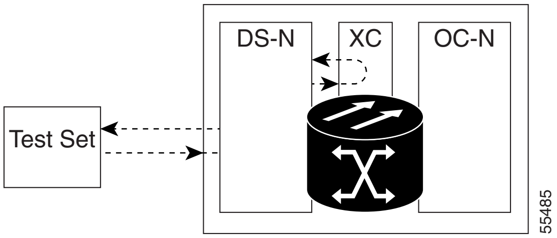
The facility (line) loopback test is performed on the node source port in the network circuit, in this example, the DS-N port in the source node. Completing a successful facility (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-10 shows an example of a facility loopback on a source DS-N port.

Figure 1-8 A Facility (Line) Loopback on a Circuit Source DS-N Port



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 1-9 shows the hairpin circuit process on a DS-N card.

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



A cross-connect loopback tests a circuit path as it passes through the cross-connect card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel at supported payloads at the STS-1 granularity and higher. For example, you can loop back a single STS-1, STS-3c, STS-6c, etc. on an optical facility (line) without interrupting the other STS circuits.

The following restrictions apply to cross-connect loopbacks:

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

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

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

The example in this section tests 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 sample scenario:

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

West to east direction (left to right):

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

East to west direction (right to left):

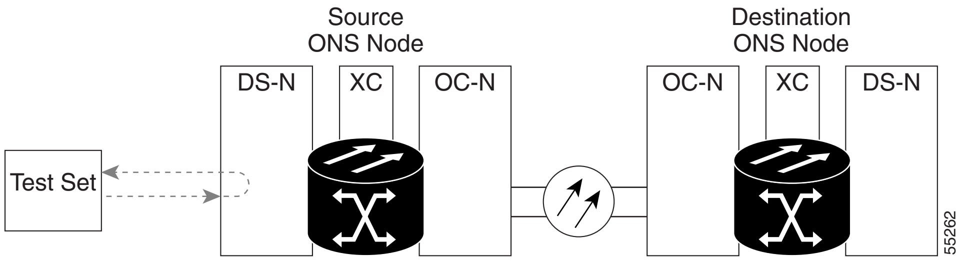
1. A facility (line) loopback on the destination node DS-N
2. A hairpin on the destination node DS-N
3. An XC loopback on the source node OC-N STS (carrying the DS-N circuit)
4. A terminal (inward) loopback on the source node DS-N

Note All loopback tests require on-site personnel.

1.3.1 Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)

The facility (line) 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 (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-10 shows an example of a facility loopback on a source DS-N port.

Figure 1-10 A Facility (Line) Loopback on a Circuit Source DS-N Port



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

Note DS-3 facility (line) loopbacks do not transmit an alarm indication signal (AIS) condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Facility (Line) 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 Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port. Adjust the test set accordingly.

Step 2 In node view, double-click the DS-N card to open the card view.

Step 3 Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 4 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.

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

Step 6 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (DS1, DS3)" condition on page 2-141 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-9.

Test and Clear the Facility (Line) Loopback Circuit

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

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

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

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

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

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 10 Complete the "Test the DS-N Cabling" procedure on page 1-10.

Test the DS-N Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

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

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

Step 3 Replace the defective cable.

Step 4 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty card or a faulty EIA.

Step 10 Complete the "Test the DS-N Card" procedure on page 1-10.

Test the DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 7 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 8 Click **Apply**.

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

Step 10 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty EIA.

Step 11 Complete the "Test the EIA" procedure on page 1-11.

Test the EIA

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

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 an Electrical Interface Assembly" procedure on page 3-17.

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

Step 3 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 5 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 6 Click **Apply**.

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

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

Step 9 Replace the faulty EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

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

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

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

Step 13 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 14 Click **Apply**.

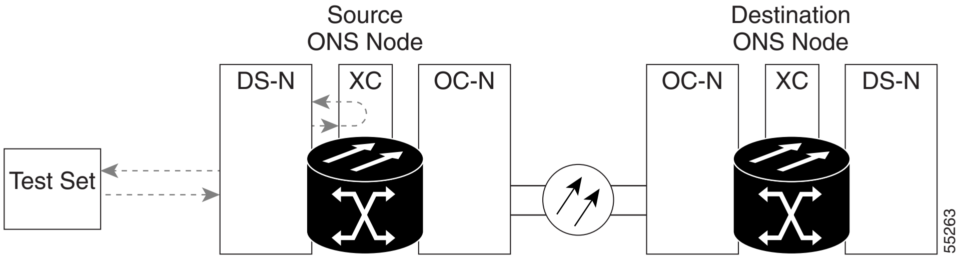
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12.

1.3.2 Perform a Hairpin Test on a Source Node Port (West to East)

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the port isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-11 shows an example of a hairpin loopback on a source node port.

Figure 1-11 Hairpin on a Source Node Port



Note The ONS 15454 does not support simplex operation on the XC10G cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Create the Hairpin Circuit 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 (Line) Loopback on a Source DS-N Port (West to East)" procedure 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 Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The Tx and Rx terminals connect to the same port.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

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

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

c. Click **Next**.

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

e. Uncheck the **Bidirectional** check box.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab and that the **Dir** column describes it as a one-way circuit.

Step 4 Complete the "Test and Delete the Hairpin Circuit" procedure on page 1-13.

Test and Delete 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:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a faulty circuit, there might be a problem with the XC10G card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-13.

Test the Standby XC10G Cross-Connect Card

Note Two XC10G cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby XC10G cross-connect card to make it the active card:

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

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

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

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

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

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby XC10G cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

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

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

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

Note After the active XC10G cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 5 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 6 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-14.

Retest the Original XC10G Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the XC10G cross-connect cards:

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

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

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

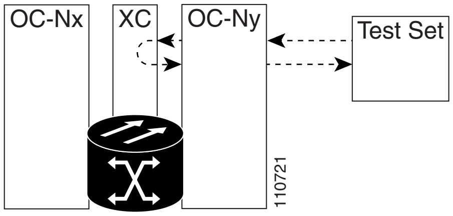
Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18.

1.3.3 Perform an XC Loopback on a Destination Node OC-N STS (West to East)

The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. The loopback occurs on the XC10G cross-connect card in a network circuit. Figure 1-12 shows an example of an XC loopback on a destination OC-N port.

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

Figure 1-12 XC Loopback on a Destination OC-N Port



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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-40, leave the optical test set hooked up to the destination node port.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

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

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the State tab.

d. Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning > SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Provisioning > SONET STS** tabs.

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

c. Click **Apply**.

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

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

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

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

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

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

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

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

Caution Cross-connect side switches 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. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

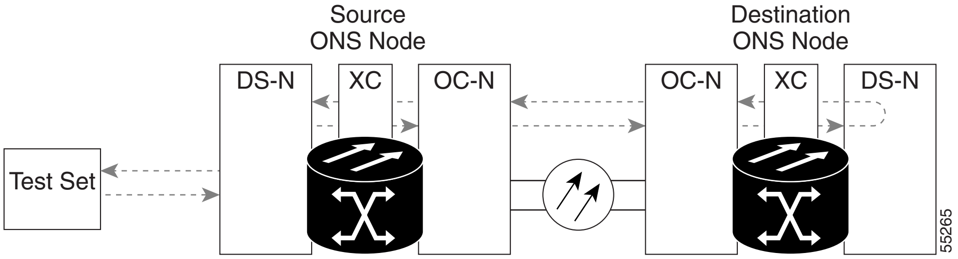
d. Click **Yes** in the Delete Circuits dialog box.

1.3.4 Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)

The terminal (inward) loopback test is performed on the node destination port in the circuit, such as a destination node DS-N port. You create a bidirectional circuit that starts on the source node DS-N port and loops back on the destination node DS-N port. Then you proceed with the terminal loopback test.

Completing a successful terminal loopback to a destination node DS-N port verifies that the circuit is good to the destination DS-N. Figure 1-13 shows an example of a terminal loopback on a destination DS-N port.

Figure 1-13 Terminal (Inward) Loopback on a Destination DS-N Port



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

Note DS-3 terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Terminal (Inward) 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 Test on a Source Node Port (West to East)" procedure on page 1-12, leave the electrical test set hooked up to the DS-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 In CTC node view, click the **Circuits** tab and click **Create**.

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

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "DS-NtoDS-N."

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

Step 7 Click **Next**.

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

Step 9 Click **Next**.

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

Step 11 Click **Finish**.

Step 12 Confirm that the newly created circuit appears in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Note DS-3 terminal loopbacks do not transmit a DS-3 AIS (see the "AIS" condition on page 2-21) in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

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

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

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

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

c. Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

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

f. Click **Apply**.

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

Step 14 Complete the "Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port" procedure on page 1-20.

Test and Clear the Terminal (Inward) 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. Double-click the DS-N card in the destination node with the terminal loopback.

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

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

Step 6 Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 11 Complete the "Test the Destination DS-N Card" procedure on page 1-21.

Test the Destination DS-N Card

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective DS-N card.

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

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

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

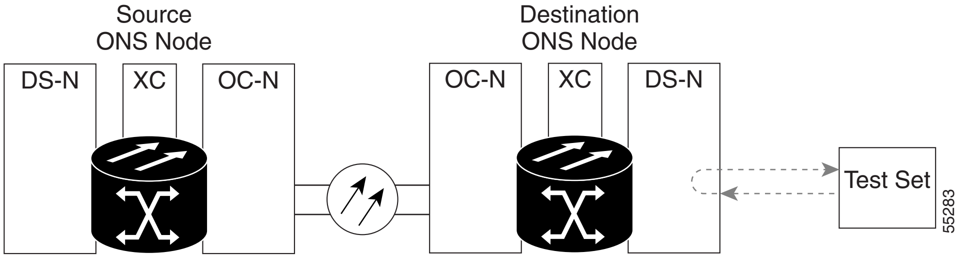
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25.

1.3.5 Perform a Facility (Line) Loopback on a Destination DS-N Port (East to West)

The facility (line) loopback test is performed on the node destination port in the network circuit, in this example, the DS-N port in the destination node. Completing a successful facility (line) loopback on this port isolates the cabling, the DS-N card, and the EIA as possible failure points. Figure 1-14 shows an example of a facility loopback on a destination DS-N port.

Figure 1-14 A Facility (Line) Loopback on a Circuit Destination DS-N Port



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

Note DS-3 facility (line) loopbacks do not transmit an alarm indication signal (AIS) condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Facility (Line) Loopback on the Destination DS-N Port

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

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

Step 2 In CTC node view, double-click the DS-N card to open the card view.

Step 3 Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

Step 4 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.

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

Step 6 Click **Apply**.

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

Note It is normal for a "LPBKFACILITY (DS1, DS3)" condition on page 2-141 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-9.

Test and Clear the Facility (Line) Loopback Circuit

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

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

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

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

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

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

Step 10 Complete the "Test the DS-N Cabling" procedure on page 1-10.

Test the DS-N Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.

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

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

Step 3 Replace the defective cable.

Step 4 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 6 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty card or a faulty EIA.

Step 10 Complete the "Test the DS-N Card" procedure on page 1-10.

Test the DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 7 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 8 Click **Apply**.

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

Step 10 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12. If the test set indicates a faulty circuit, the problem might be a faulty EIA.

Step 11 Complete the "Test the EIA" procedure on page 1-11.

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 an Electrical Interface Assembly" procedure on page 3-17.

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

Step 3 In card view for the DS-N card, depending upon the type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

Step 5 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 6 Click **Apply**.

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

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

Step 9 Replace the faulty EIA. See the "Replace an Electrical Interface Assembly" procedure on page 3-17.

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

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

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

Step 13 Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

Step 14 Click **Apply**.

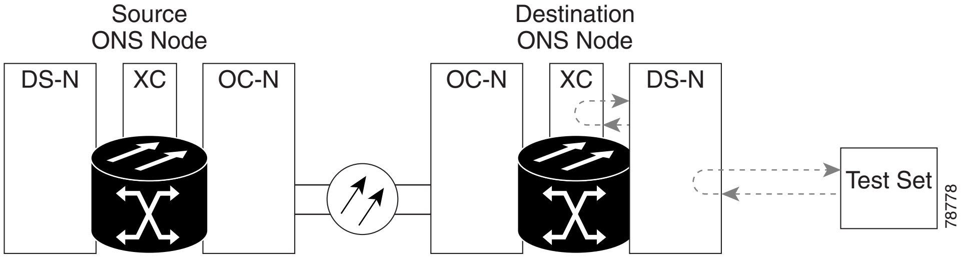
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "Perform a Hairpin Test on a Source Node Port (West to East)" procedure on page 1-12.

1.3.6 Perform a Hairpin Test on a Destination Node Port (East to West)

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 1-15 shows an example of a hairpin loopback on a destination node port.

Figure 1-15 Hairpin on a Destination Node Port



Note The ONS 15454 does not support simplex operation on the XC10G cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Create the Hairpin Circuit on the Destination Node Port

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

- **a.** If you just completed the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8, 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 Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The Tx and Rx terminals connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

- **a.** In node view, click the **Circuits** tab and click **Create**.
- **b.** In the Circuit Creation dialog box, choose the type and size, such as an STS-1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "Hairpin1."
- **e.** Uncheck the **Bidirectional** check box.
- **f.** Click **Next**.
- **g.** In the Circuit Creation source dialog box, select the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.
- **h.** Click **Next**.
- **i.** In the Circuit Creation destination dialog box, use the same **Node**, card **Slot**, **Port**, and **STS** (or **VT**) used for the source dialog box.
- **j.** Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab and that the **Dir** column describes it as a one-way circuit.

Step 4 Complete the "Test and Delete the Hairpin Circuit" procedure on page 1-13.

Test and Delete 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:

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

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a faulty circuit, there might be a problem with the XC10G card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-13.

Test the Standby XC10G Cross-Connect Card

Note Two XC10G cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby XC10G cross-connect card to make it the active card:

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

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

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

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

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

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby XC10G cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

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

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

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

Note After the active XC10G cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 5 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 6 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-14.

Retest the Original XC10G Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the XC10G cross-connect cards:

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

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

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

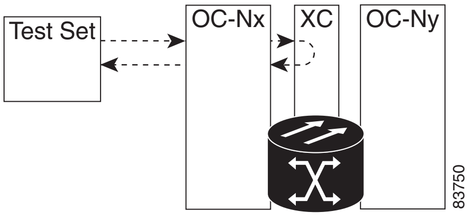
Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Destination DS-N Port (West to East)" procedure on page 1-18.

1.3.7 Perform an XC Loopback on a Source Node OC-N STS (East to West)

The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. It also eliminates the cross-connect card as the source of trouble for a faulty circuit. The loopback occurs on the XC10G cross-connect card in a network circuit. Figure 1-16 shows an example of an XC loopback on a source OC-N port.

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

Figure 1-16 XC Loopback on a Source OC-N Port



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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-40, leave the optical test set hooked up to the source node port.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

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

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the State tab.

d. Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning > SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Provisioning > SONET STS** tabs.

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

c. Click **Apply**.

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

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

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

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

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

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

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

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

Caution Cross-connect side switches 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. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

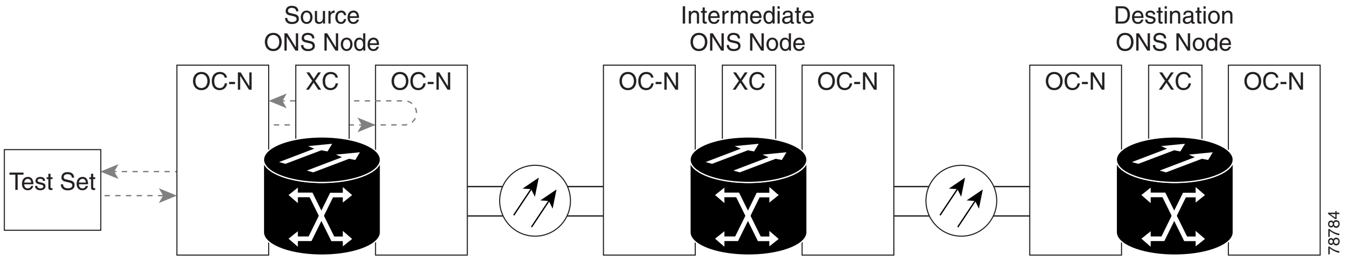
c. Click **Delete**.

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

1.3.8 Perform a Terminal (Inward) Loopback on a Source DS-N Port (East to West)

The terminal (inward) loopback test is performed on the node source port in the circuit, such as a source node DS-N port. You first create a bidirectional circuit that starts on the destination node DS-N port and loops back on the source node DS-N port. Then you proceed with the terminal loopback test. Completing a successful terminal loopback to a source node DS-N port verifies that the circuit is good to the source DS-N. Figure 1-17 shows an example of a terminal loopback on a source DS-N port.

Figure 1-17 Terminal (Inward) Loopback on a Source DS-N Port



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

Note DS-3 terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

Create the Terminal (Inward) Loopback on a Source 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 Test on a Source Node Port (West to East)" procedure on page 1-12, leave the electrical test set hooked up to the DS-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 In CTC node view, click the **Circuits** tab and click **Create**.

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

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "DS-NtoDS-N."

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

Step 7 Click **Next**.

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

Step 9 Click **Next**.

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

Step 11 Click **Finish**.

Step 12 Confirm that the newly created circuit appears in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

Note DS-3 terminal loopbacks do not transmit a DS-3 AIS (see the "AIS" condition on page 2-21) in the direction away from the loopback. Instead of a DS-3 AIS, a continuance of the signal transmitted to the loopback is provided.

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

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

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

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

c. Depending upon the card type, click the **Maintenance > Loopback** tabs, **Maintenance > DS1** tabs, or **Maintenance > DS3** tabs.

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

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

f. Click **Apply**.

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

Step 14 Complete the "Test and Clear the Terminal (Inward) Loopback Circuit on the Destination DS-N Port" procedure on page 1-20.

Test and Clear the Terminal (Inward) Loopback Circuit on the Source 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. Double-click the DS-N card in the destination node with the terminal loopback.

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

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

Step 6 Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 11 Complete the "Test the Destination DS-N Card" procedure on page 1-21.

Test the Destination DS-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective DS-N card.

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

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

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

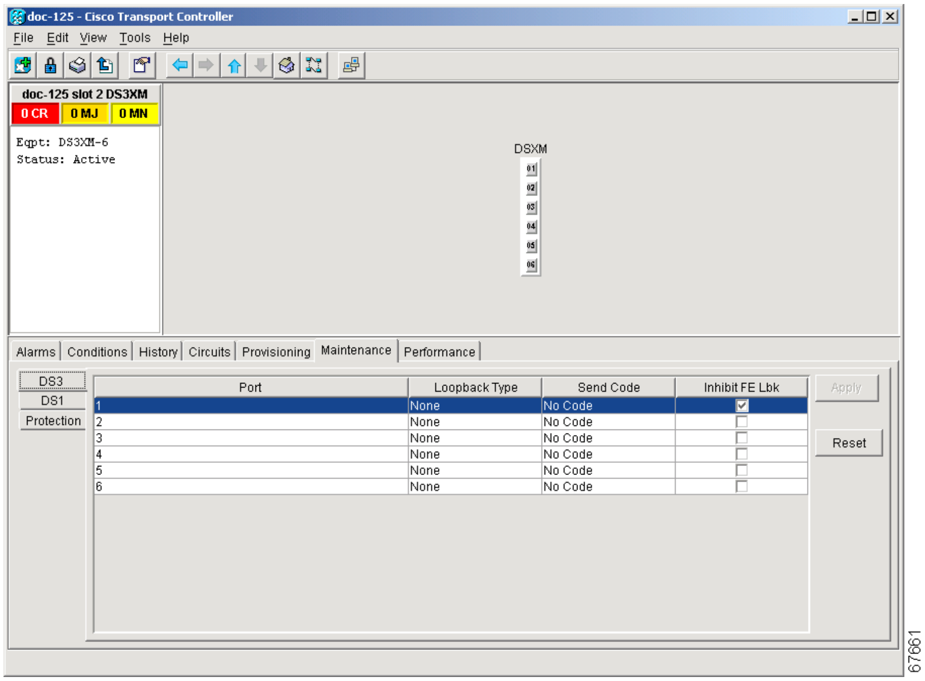
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Hairpin Test on a Destination Node Port (East to West)" procedure on page 1-25.

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

The DS3XM-6 card supports far-end access 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 1-18 shows the DS3 subtab and the additional Send Code and Inhibit FE Lbk function columns.

Figure 1-18 Accessing FEAC Functions on the DS3XM-6 Card

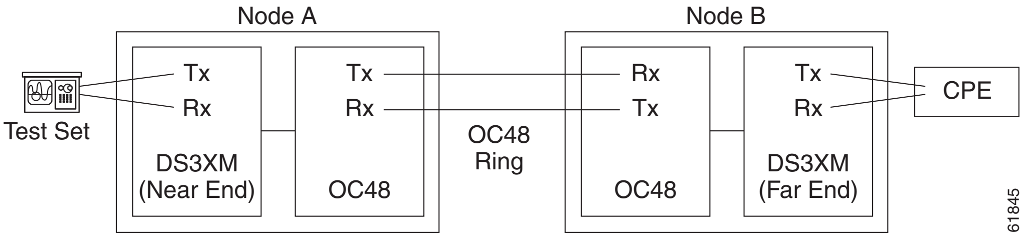


Eqpt: DS3XM-6
Status: Active

Port	Loopback Type	Send Code	Inhibit FE Lbk
1	None	No Code	☑
2	None	No Code	□
3	None	No Code	□
4	None	No Code	□
5	None	No Code	□
6	None	No Code	□

The “far end” in FEAC refers to the equipment connected to the DS3XM-6 card and not to the far end of a circuit. In Figure 1-19, 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 1-19 Diagram of FEAC



1.4.1 FEAC Send Code

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

1.4.2 DS-3I Inhibit Loopback

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

1.4.3 DS3XM-6 Inhibit FEAC Loopback

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

1.4.4 FEAC Alarms

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

1.5 Identify Points of Failure on an Optical Circuit Path

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

You can use these procedures on OC-N cards, G-Series Ethernet cards, transponder (TXP, TXPP) cards, and muxponder (MXP) cards. The example in this section tests an OC-N circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains seven network test procedures:

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

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

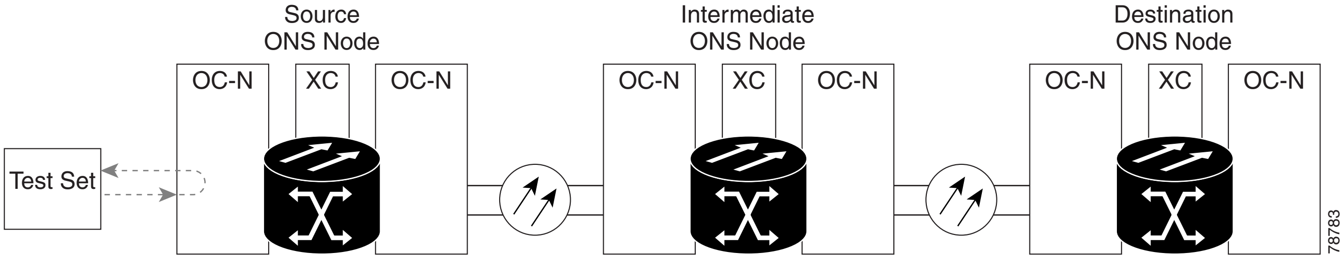
Note All loopback tests require on-site personnel.

1.5.1 Perform a Facility (Line) Loopback on a Source-Node G-Series, MXP, OC-N, or TXP Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source OC-N port in the source node. Completing a successful facility (line) loopback on this port isolates the OC-N port as a possible failure point. Figure 1-20 shows an example of a facility loopback on a circuit source OC-N port. G-Series Ethernet ports, TXPs, and MXPs are tested similarly.

Note Facility (line) loopbacks are not available for G-Series cards prior to software R4.1.

Figure 1-20 Facility (Line) Loopback on a Circuit Source OC-N Port



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

Create the Facility (Line) Loopback on the Source Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

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

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

Step 3 Click the **Maintenance > Loopback** tabs.

Step 4 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.

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

Step 6 Click **Apply**.

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

> **Note** It is normal for a "LPBKFACILITY (OCN)" condition on page 2-142, or a "LPBKFACILITY (G1000)" condition on page 2-142 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-39.

Test and Clear the Facility (Line) Loopback Circuit

> **Note** This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

Step 4 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-39.

Test the OC-N, G-Series, MXP, or TXP Card

> **Note** This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40.

1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port

The terminal (inward) loopback test is performed on the node source OC-N, G-Series, MXP, or TXP port. For the circuit in this example, it is the source OC-N port in the source node. You first create a bidirectional circuit that starts on the node destination OC-N port and loops back on the node source OC-N port.You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-21 shows an example of a terminal loopback on a source OC-N port.

Note Terminal (inward) loopbacks are not available for E-Series Ethernet, ML-Series Ethernet, and DWDM cards in R4.6.

Note Terminal (inward) loopbacks are not available for G-Series cards prior to R4.0.

Figure 1-21 Terminal (Inward) Loopback on a Source-Node OC-N Port

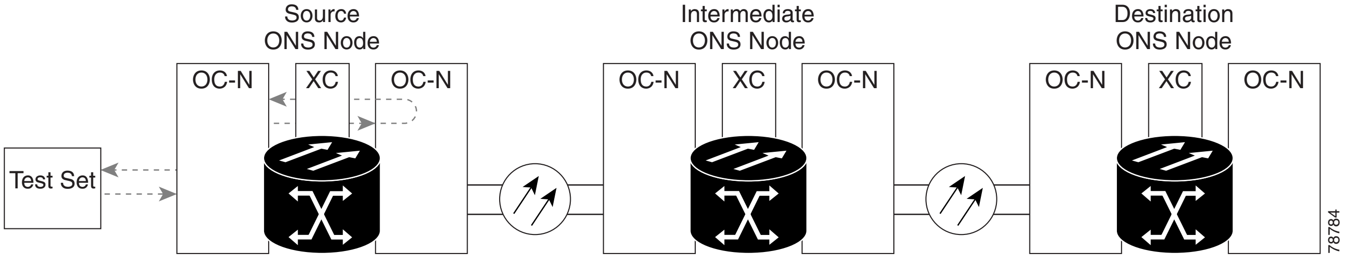
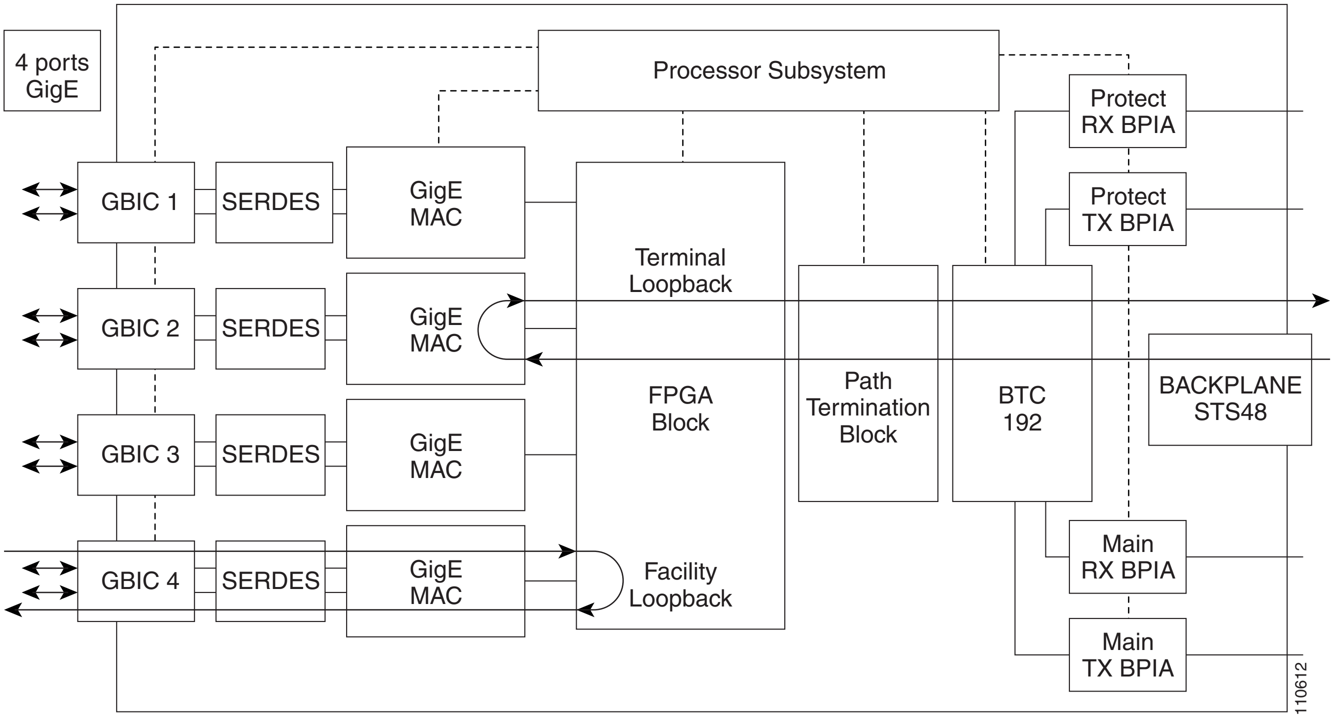


Figure 1-22 shows terminal loopback on a G-Series card.

Figure 1-22 Terminal (Inward) Loopback on a G-Series Port



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

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

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node G-Series, MXP, OC-N, or TXP Port" procedure on page 1-38, leave the optical test set hooked up to the OC-N, G-Series, MXP, or TXP port in the source node.

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

c. Adjust the test set accordingly.

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

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

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

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCN2."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

b. Click the **Maintenance > Loopback** 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 **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-42.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-43.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective card.

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

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

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

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

a. Click the **Circuits** tab.

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

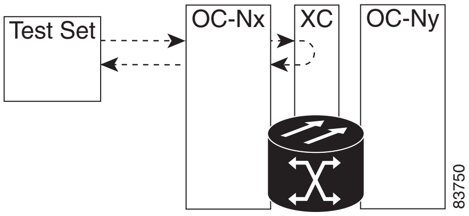
Step 7 Complete the "Create the XC Loopback on the Source OC-N Port" procedure on page 1-44.

1.5.3 Create the XC Loopback on the Source OC-N Port

Note This procedure is only performed on OC-N cards and tests the XC-10G circuit connection.

The cross-connect (XC) loopback test occurs on the XC10G cross-connect card in a network circuit. Completing a successful XC loopback from an OC-N card through the cross-connect card eliminates the cross-connect card as the source of trouble for a faulty circuit. Figure 1-23 shows an example of an XC loopback on a source OC-N port.

Figure 1-23 XC Loopback on a Source OC-N Port



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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

- **a.** If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40, leave the optical test set hooked up to the source node port.
- **b.** If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. The Tx and Rx terminals connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

- **a.** In node view, click the **Circuits** tab.
- **b.** Click the circuit and then click **Edit**.
- **c.** In the Edit Circuit dialog box, click the State tab.
- **d.** Choose **OOS-MT** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 3 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the OC-N card to open the card view.

b. Click the **Provisioning > SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the XC Loopback Circuit" procedure on page 1-45.

Test the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Provisioning > SONET STS** tabs.

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

c. Click **Apply**.

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

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-48. If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Complete the "Test the Standby XC10G Cross-Connect Card" procedure on page 1-45.

Test the Standby XC10G Cross-Connect Card

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

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

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

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

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

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

Caution Cross-connect side switches 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. On both the physical node and the CTC node view window, the standby cross-connect's ACT/SBY LED is amber and the active card's ACT/SBY LED is green.

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC10G Cross-Connect Card" procedure on page 1-46.

Retest the Original XC10G Cross-Connect Card

Note This procedure is performed only on OC-N and XC10G cards.

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447) and proceed to Step 4. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 4 Complete the "Replace an In-Service Cross-Connect Card" procedure on page 3-2 for the defective cross-connect card and perform Step 5.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

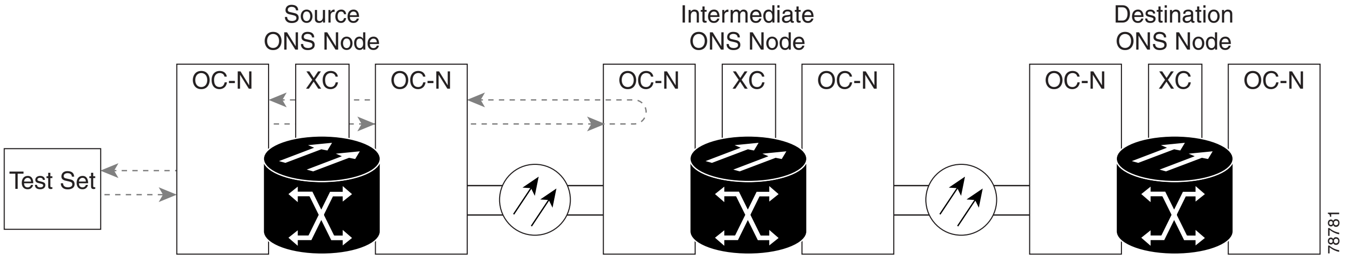
c. Click **Delete**.

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

1.5.4 Create a Facility (Line) Loopback on an Intermediate-Node G-Series, MXP, OC-N, or TXP Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-24, the test is being performed on an intermediate OC-N port.

Figure 1-24 Facility (Line) Loopback on an Intermediate-Node OC-N Port



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

Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-40, leave the optical test set hooked up to the source node port.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility (line) loopback on the test port:

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

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

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn3."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-142, or the "LPBKFACILITY (OCN)" condition on page 2-142 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility (line) loopback on the destination port being tested:

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

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

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-49.

Test and Clear the Facility (Line) Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51. If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-50.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

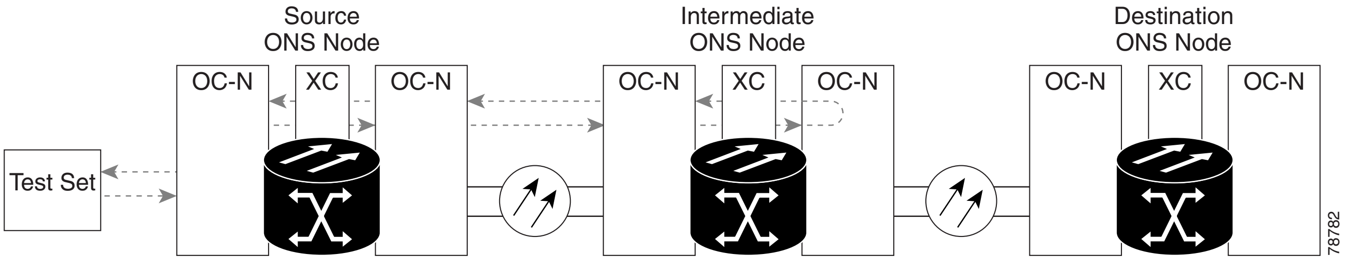
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51.

1.5.5 Create a Terminal (Inward) Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-25, the terminal loopback is performed on an intermediate OC-N port in the circuit. You first create a bidirectional circuit that originates on the source node OC-N, G-Series, MXP, or TXP port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-25 Terminal Loopback on an Intermediate-Node OC-N Port



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

Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "Create a Facility (Line) Loopback on an Intermediate-Node OC-N, G-Series, MXP, or TXP Port" section on page 1-48, leave the optical test set hooked up to the source node port.

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

c. Adjust the test set accordingly.

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

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

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

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn4."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the **Dir** column as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-52.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

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

d. Select the appropriate state (IS, OOS, OOS_AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

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

Step 5 Complete the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-53.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

Step 6 Clear the terminal loopback circuit:

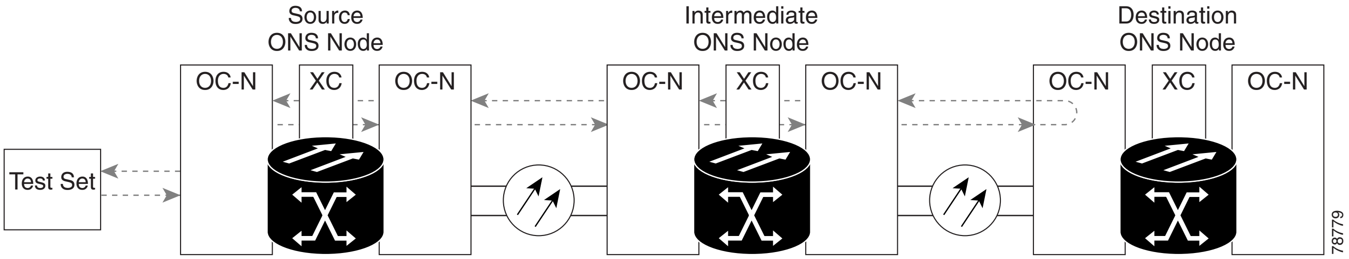
- **a.** Click the **Circuits** tab.
- **b.** Choose the loopback circuit being tested.
- **c.** Click **Delete**.
- **d.** Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54.

1.5.6 Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-26 shows a facility loopback being performed on an OC-N port, but you can also use this procedure on G-Series, MXP, or TXP cards.

Figure 1-26 Facility (Line) Loopback on a Destination Node OC-N Port



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

Create the Facility (Line) Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "Create a Terminal Loopback on Intermediate-Node OC-N, G-Series, MXP, or TXP Ports" procedure on page 1-51, leave the optical test set hooked up to the source node port.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin circuit on the test port:

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

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

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn5."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for a "LPBKFACILITY (G1000)" condition on page 2-142, or a "LPBKFACILITY (OCN)" condition on page 2-142 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility (line) loopback on the destination port being tested:

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

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

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-49.

Test and Clear the Facility (Line) Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-57. If the test set indicates a faulty circuit, the problem might be a faulty OC-N card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-50.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the faulty card.

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

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

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

c. Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

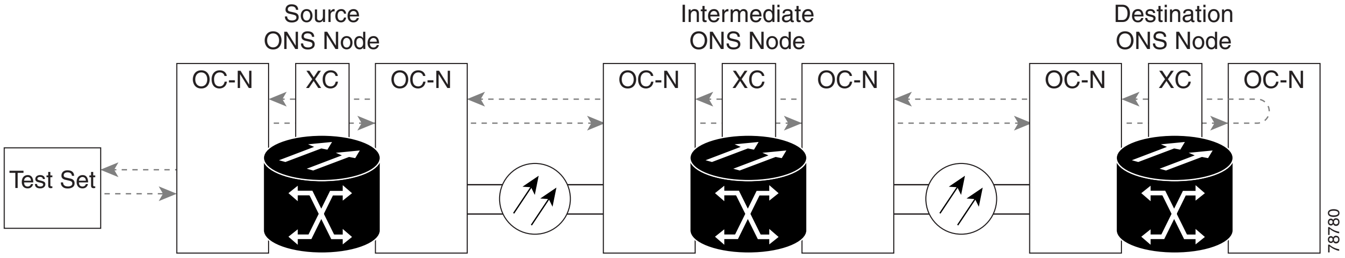
d. Click **Yes** in the Delete Circuits dialog box.

Step 7 Complete the "Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-57.

1.5.7 Perform a Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port

The terminal loopback at the destination node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-27 shows a terminal loopback on an intermediate node destination OC-N port.

Figure 1-27 Terminal Loopback on a Destination Node OC-N Port



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

Create the Terminal Loopback on a Destination Node OC-N, G-Series, MXP, or TXP Port

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

Note Refer to the manufacturer's instructions for detailed information about connection and setup of the optical test set.

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node OC-N, G-Series, MXP, or TXP Port" procedure on page 1-54, leave the optical test set hooked up to the source port.

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

c. Adjust the test set accordingly.

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

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

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

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as "OCn1toOCn6."

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

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

h. Click **Next**.

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

j. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a 2-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)" condition on page 2-144 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-58.

Test and Clear the Terminal Loopback Circuit

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

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

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

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

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

Step 4 Clear the terminal loopback circuit:

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

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

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the OC-N, G-Series, MXP, or TXP Card" procedure on page 1-59.

Test the OC-N, G-Series, MXP, or TXP Card

Note This procedure does not apply to Software R4.6 E-Series Ethernet, ML-Series Ethernet, and DWDM cards.

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the suspected bad card and replace it with a known-good card.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-219 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

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

1.6 Restoring the Database and Default Settings

This section contains troubleshooting for node operation errors that require restoration of software data or the default node setup.

1.6.1 Restore the Node Database

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

Table 1-2 describes the potential causes of the symptom and the solution.

Table 1-2 Restore the Node Database

Possible Problem	Solution
Incorrect or corrupted node database.	Perform a Restore the Database procedure. Refer to the "Restore the Database" procedure on page 1-60.

Restore the Database

Note The following parameters are not backed up and restored: node name, IP address, subnet mask and gateway, and Internet Inter-ORB Protocol (IIOP) port. If you change the node name and then restore a backed up database with a different node name, the circuits 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 reconvergence. The CARLOSS (E100T, E1000F) alarm appears and clears during this period.

Caution If you are restoring the database on multiple nodes, wait approximately one minute after the TCC2 reboot has completed on each node before proceeding to the next node.

Step 1 In CTC, 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 appear 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 appears.

c. In the Login dialog box, type a user name and password (both are case sensitive) and click **Login**. The CTC node view window appears.

Step 2 Ensure that no ring or span (four-fiber only) switch events are present; for example, ring-switch east or west and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.

Step 3 If switch events need to be cleared, in node view click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

a. If a switch event (not caused by a line failure) is present, choose **CLEAR** from the drop-down menu and click **Apply**.

b. If a switch event caused by the Wait to Restore (WTR) condition is present, choose **LOCKOUT SPAN** from the drop-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the drop-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 hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15454 software CD.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup might 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 TCC2.

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.

1.6.2 Restore the Node to Factory Configuration

Symptom A node has both TCC2 cards in standby state, and you are unable reset the TCC2 cards to make the node functional.

Table 1-3 describes the possible problems and the solution.

Table 1-3 Restore the Node to Factory Configuration

Possible Problem	Solution
Failure of both TCC2 cards in the node.	Restore the node to factory configuration. Refer to the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-63 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-64 as required.
Replacement of both TCC2 cards at the same time.	

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses 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 might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution If you are restoring the database on multiple nodes, wait until the TCC2 cards have rebooted on each node before proceeding to the next node.

Caution Restoring a node to factory configuration on a Windows or UNIX workstation should only be carried out on a standby TCC2 card.

Caution Cisco recommends that you take care to save the node database to a safe location if you will not be restoring the node using the database provided on the software CD.

Note The following parameters are not backed up and restored when you delete the database and restore the factory settings: node name, IP address, subnet 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 map to the new renamed node. Cisco recommends keeping a record of the old and new node names.

Note If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-28 on page 1-63).

Note If you need to install or replace one or more TCC2 cards, refer to the *Cisco ONS 15454 Procedure Guide* for installation instructions.

Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Restoring a node to factory configuration on a Windows workstation should only be carried out on a standby TCC2 card.

Note The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

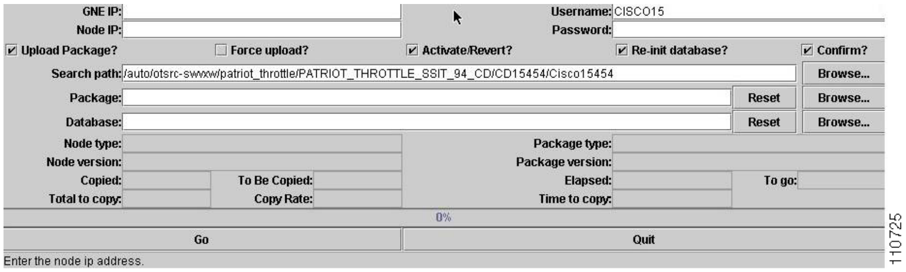
Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

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 choose **All Files from the Files of Type** drop-down menu.

Step 4 Select the RE-INIT.jar file and click **Open** to open the reinit tool (Figure 1-28).

Figure 1-28 Reinitialization Tool in Windows



GNE IP:
Node IP:
Username: CISCO15
Password:

☑ Upload Package? ☐ Force upload? ☑ Activate/Revert? ☑ Re-init database? ☑ Confirm?

Search path: /auto/otsrc-swxw/patriot_throttle/PATRIOT_THROTTLE_SSIT_94_CD/CD15454/Cisco15454

Package:
Database:
Node type:
Node version:
Package type:
Package version:
Copied:
To Be Copied:
Elapsed:
To go:
Total to copy:
Copy Rate:
Time to copy:

0%

Enter the node ip address.

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 1-28).

Step 7 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 8 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 9 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.6 when version 4.6 is already active), check the Force Upload checkbox.This option forces the NE to have the same software version on the working and protect flash memory.

Note The Force Upload box is only applicable when the Upload Package checkbox is checked.

Step 10 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

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 11 Click **Go**. A confirmation dialog box appears.

Step 12 Click **Yes**.

Step 13 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC2 successfully uploaded the database, not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

Step 14 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 TCC2 card 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.

Step 15 Manually set the node name and network configuration to site-specific values. See the *Cisco ONS 15454 Procedure Guide* for information about setting the node name, IP address, mask and gateway, and IIOP port.

Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Restoring a node to factory configuration on a UNIX workstation should only be carried out on a standby TCC2 card.

Note The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

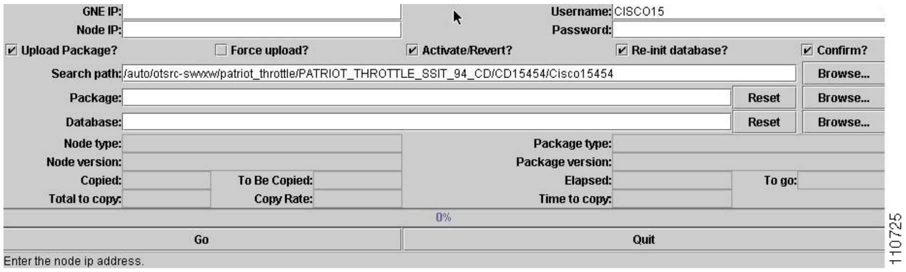
Note Java Runtime Environment (JRE) 1.03_02 must also be installed on the computer you use to perform this procedure.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, 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 1-29). If you are working with a command line interface, run **java -jar RE-INIT.jar**.

Figure 1-29 Reinitialization Tool in UNIX



GNE IP:
Node IP:
Username: CISCO15
Password:

☑ Upload Package? ☐ Force upload? ☑ Activate/Revert? ☑ Re-init database? ☑ Confirm?

Search path: /auto/otsrc-swxw/patriot_throttle/PATRIOT_THROTTLE_SSIT_94_CD/CD15454/Cisco15454
Package:
Database:

Node type:
Node version:
Package type:
Package version:
Copied:
To Be Copied:
Elapsed:
To go:
Total to copy:
Copy Rate:
Time to copy:

0%

Enter the node ip address.

Step 4 If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-29).

Step 6 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 7 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 8 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.6 when version 4.6 is already active), check the Force Upload checkbox. This option forces the NE to have the same software version on the working and protect flash memory.

Step 9 In the Search Path field, verify that the path to the CISCO15454 folder on the CD-ROM drive is listed.

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 10 Click **Go**. A confirmation dialog box appears.

Step 11 Click **Yes**.

Step 12 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC2 successfully uploaded the database; not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

Step 13 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 TCC2 card or on the hub or switch where the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

Step 14 Set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedure Guide* for information about provisioning the node name, IP address, subnet mask and gateway, and IIOP port.

1.7 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R4.6, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.7.1 PC System Minimum Requirements

Workstations running CTC R4.6 for the ONS products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space
- 20 GB or larger hard drive

1.7.2 Sun System Minimum Requirements

Workstations running CTC R4.6 for the ONS products on Sun workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space

1.7.3 Supported Platforms, Browsers, and JREs

Software R4.6 CTC supports the following platforms:

- Windows NT
- Windows 98
- Windows XP
- Windows 2000
- Solaris 8
- Solaris 9

Software R4.6 CTC supports the following browsers and JREs:

- Netscape 4.76 (on Solaris 8 or 9 with Java plug-in 1.3.1)
- Netscape 7 (on Solaris 8 or 9 with Java plug-in 1.4)

- PC platforms with Java plug-in 1.3.1 or 1.4
- Internet Explorer 6.0 (on PC platforms with Java plug-in 1.3.1 or 1.4)

Note You can obtain browsers at the following URLs:
Netscape: http://channels.netscape.com/ns/browsers/default.jsp
Internet Explorer: http://www.microsoft.com

Note The recommended JRE version is JRE 1.4.2.

Note JRE 1.4.2 for Windows and Solaris is available on R4.6 product CDs.

1.7.4 Unsupported Platforms and Browsers

Software R4.6 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R4.6 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris is not supported except when used with JRE 1.3.1.
- JRE 1.4.2 is not supported except with Netscape 7 on Solaris 8 or 9.

1.7.5 Unable to Verify the IP Configuration of Your PC

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

Table 1-4 on page 1-67 describes the possible problems and the solutions.

Table 1-4 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. See the "Verify the IP Configuration of Your PC" procedure on page 1-68.
The IP configuration of your PC is not properly set.	Verify the IP configuration of your PC. Complete the "Verify the IP Configuration of Your PC" procedure on page 1-68. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

Step 1 Open a DOS command window by selecting **Start > Run** from the Start menu.

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

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

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

The Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.

Note The winipcfg command only returns the information above if you are on a network.

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

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

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

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

1.7.6 Browser Login Does Not Launch Java

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

Table 1-5 describes the possible problem and the solution.

Table 1-5 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. Complete the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-68 and the "Reconfigure the Browser" procedure on page 1-69.

Reconfigure the PC Operating System Java Plug-in Control Panel

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

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

a. Run the Cisco ONS 15454 software CD.

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

c. Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.

d. Follow the JRE installation wizard steps.

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

Step 4 In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.

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

Step 6 Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

Step 7 Select **JRE 1.4**.

Step 8 Click **Apply**.

Step 9 Close the Java Plug-in Control Panel window.

Reconfigure the Browser

Step 1 From the Start Menu, launch your browser application.

Step 2 If you are using Netscape Navigator:

a. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

b. In the Preferences window, click the **Advanced > Proxies** categories.

c. In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.

d. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

e. In the Preferences window, click the **Advanced > Cache** categories.

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Windows 98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**
- For Windows NT/2000, **C:\ProgramFiles\Netscape\***username***\Communicator\cache**.

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

h. Navigate to the file listed in Step f, and click **OK**.

i. Click **OK** on the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

a. On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

b. In the Internet Options window, click the **Advanced** tab.

c. In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for** *applet* **(requires restart)** check box.

d. Click **OK** in the Internet Options window and exit the browser.

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.8.3 Browser Stalls When Downloading CTC JAR Files From TCC2" section on page 1-74.

Step 5 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 6 Restart the browser and log on to the ONS 15454.

1.7.7 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 1-6 describes the possible problems and the solutions.

Table 1-6 Unable to Verify the NIC Connection on your PC

Possible Problem	Solution
The CAT-5 cable is not plugged in properly.	Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.
The CAT-5 cable is damaged.	Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending.
Incorrect type of CAT-5 cable is being used.	If connecting an ONS 15454 directly to your laptop, a 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 CAT-5 cables, see the "1.10.2.1 Crimp Replacement LAN Cables" section on page 1-97.
The NIC is improperly inserted or installed.	If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. If the NIC is built into the laptop or PC, verify that the NIC is not faulty.
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 might be faulty and needs to be replaced.

1.7.8 Verify PC Connection to the ONS 15454 (ping)

Symptom The TCP/IP connection was established and then lost.

Table 1-7 describes the possible problem and the solution.

Table 1-7 Verify PC Connection to ONS 15454 (ping)

Possible Problem	Solution
A lost connection between the PC and the ONS 15454.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2 card. A ping command should work if the PC connects directly to the TCC2 card or uses a LAN to access the TCC2 card. Complete the "Ping the ONS 15454" procedure on page 1-71.

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** 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 198.168.10.10
```

Step 3 If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 4 If the ping is successful, 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.

1.7.9 The IP Address of the Node is Unknown

Symptom The IP address of the node is unknown and you are unable to login.

Table 1-8 describes the possible problem and the solution.

Table 1-8 Retrieve the Unknown IP Address of the Node

Possible Problem	Solution
The node is not set to the default IP address.	Leave one TCC2 card in the shelf. Connect a PC directly to the remaining TCC2 card and perform a hardware reset of the card. The TCC2 card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the "Retrieve Unknown Node IP Address" procedure on page 1-71.

Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active TCC2 card Ethernet port on the faceplate.

Step 2 Start the Sniffer application on your PC.

Step 3 Perform a hardware reset by pulling and reseating the active TCC2 card.

Step 4 After the TCC2 card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.

1.8 CTC Operation Troubleshooting

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

1.8.1 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, you are unable to launch CTC Help and receive an "MSIE is not the default browser" error message.

Table 1-9 describes the possible problem and the solution.

Table 1-9 Unable to Launch CTC Help After Removing Netscape

Possible Problem	Solution
Loss of association between browser and Help files.	When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as the default browser so that CTC associates the Help files to the correct browser. Complete the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-72 to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

Step 1 Open the Internet Explorer browser.

Step 2 From the menu bar, click **Tools** > **Internet Options**. The Internet Options window appears.

Step 3 In the Internet Options window, click the **Programs** tab.

Step 4 Click the **Internet Explorer should check to see whether it is the default browser** check box.

Step 5 Click **OK**.

Step 6 Exit any and all open and running CTC and Internet Explorer applications.

Step 7 Launch Internet Explorer and open a new CTC session. You should now be able to access the CTC Help.

1.8.2 Unable to Change Node View to Network View

Symptom When activating a large, multinode BLSR from Software R3.2 to Software R3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

Table 1-10 describes the possible problem and the solution.

Table 1-10 Browser Stalls When Downloading Files From TCC2

Possible Problem	Solution
The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.	Reset the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-73 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-73 to enable the CTC_HEAP variable change. **Note** This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

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 My Computer and choose **Properties** in the shortcut menu.

Step 3 In the System Properties window, click the **Advanced** tab.

Step 4 Click **Environment Variables** to open the Environment Variables window.

Step 5 Click **New** 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.

Restart the browser and CTC software.

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
```

Step 4 Restart the browser and CTC software in the same user shell window.

1.8.3 Browser Stalls When Downloading CTC JAR Files From TCC2

Symptom The browser stalls or hangs when downloading a CTC JAR file from the TCC2 card.

Table 1-11 describes the possible problem and the solution.

Table 1-11 Browser Stalls When Downloading JAR Files from TCC2

Possible Problem	Solution
McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.	Disable the VirusScan Download Scan feature. Complete the "Disable the VirusScan Download Scan" procedure on page 1-74.

Disable the VirusScan Download Scan

Step 1 From the Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.

Step 2 Double-click the **VShield** icon listed in the VirusScan Console dialog box.

Step 3 Click **Configure** on the lower part of the Task Properties window.

Step 4 Click the **Download Scan** icon on the left of the System Scan Properties dialog box.

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

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

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

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

Step 9 Close the McAfee VirusScan window.

1.8.4 CTC Does Not Launch

Symptom CTC does not launch; usually an error message appears before the login window appears.

Table 1-12 describes the possible problem and the solution.

Table 1-12 CTC Does Not Launch

Possible Problem	Solution
The Netscape browser cache might point to an invalid directory.	Redirect the Netscape cache to a valid directory. Complete the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-75.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 open the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

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

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

1.8.5 Slow CTC Operation or Login Problems

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

Table 1-13 describes the possible problem and the solution.

Table 1-13 Slow CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might 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. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-75 or the "Delete the CTC Cache File Manually" procedure on page 1-76.

Delete the CTC Cache File Automatically

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting CTC cache might cause any CTC running on this system to behave in an unexpected manner.

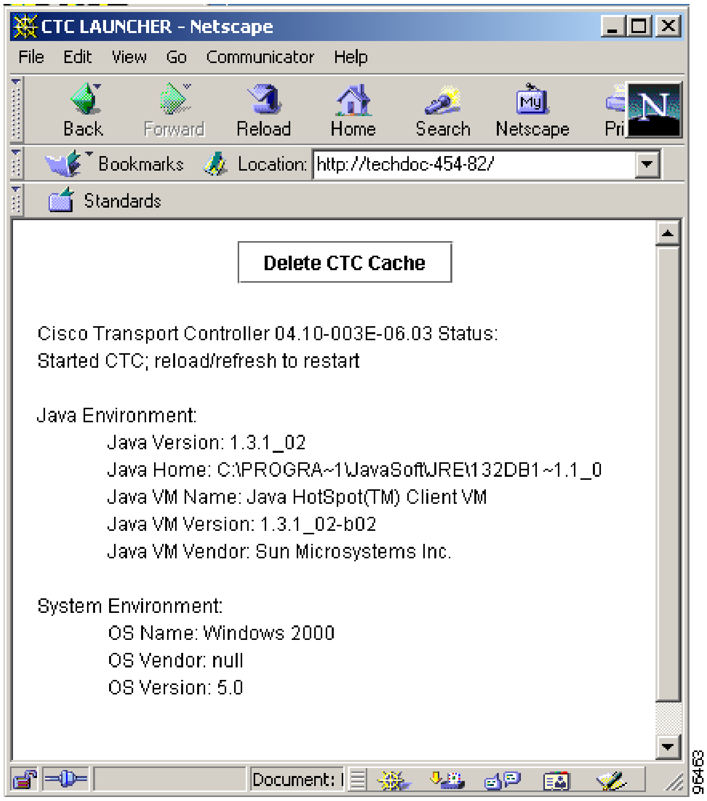
Step 1 Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2 Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.

Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-30 shows the Delete CTC Cache window.

Note For CTC releases earlier than R3.0, automatic deletion is unavailable. For CTC cache file manual deletion, complete the "Delete the CTC Cache File Manually" procedure on page 1-76.

Figure 1-30 Deleting the CTC Cache


CTC LAUNCHER - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Pri
Bookmarks Location: http://techdoc-454-82/
Standards
Delete CTC Cache
Document:
96463

Cisco Transport Controller 04.10-003E-06.03 Status:
Started CTC; reload/refresh to restart

Java Environment:
Java Version: 1.3.1_02
Java Home: C:\PROGRA~1\JavaSoft\JRE\132DB1~1.1_0
Java VM Name: Java HotSpot(TM) Client VM
Java VM Version: 1.3.1_02-b02
Java VM Vendor: Sun Microsystems Inc.

System Environment:
OS Name: Windows 2000
OS Vendor: null
OS Version: 5.0

Delete the CTC Cache File Manually

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

Step 1 To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.

Step 2 Enter *.jar in the Search for files or folders named field in the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2. These files might include CTC*.jar, CMS*.jar, and jar_cache*.tmp.

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

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

1.8.6 Node Icon is Gray on CTC Network View

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

Table 1-14 describes the possible problems and the solutions.

Table 1-14 Node Icon is Gray on CTC Network View

Possible Problem	Solution
Different CTC releases not recognizing each other.	Correct the core version build as described in the "1.8.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-80.
A username/password mismatch.	Correct the username and password as described in the "1.8.10 Username or Password Do Not Match" section on page 1-81.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.8.15 Ethernet Connections" section on page 1-83.
A lost DCC connection.	Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.8.7 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 1-15 on page 1-78 describes the possible problem and the solution.

Table 1-15 CTC Cannot Launch Due to Applet Security Restrictions

Possible Problem	Solution
You are logging into a node running CTC Software R4.0 or earlier. Releases earlier than R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.	1. Install the software CD for the release of the node you are logging into. 2. Run the CTC Setup Wizard (double-click **Setup.exe**). 3. Choose **Custom installation**, then choose the Java Policy option. For additional information, refer to the CTC installation information in the *Cisco ONS 15454 Procedure Guide*. 4. If the software CD is not available, you must manually edit the java.policy file on your computer. Complete the "Manually Edit the java.policy File" procedure on page 1-78.

Manually Edit the java.policy File

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

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

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

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

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

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as **.java.policy**. On Win98/2000 PCs, save the file to the C:\Windows folder. On Windows NT 4.0 or later PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.8.8 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Table 1-16 describes the possible problem and the solution.

Table 1-16 Java Runtime Environment Incompatible

Possible Problem	Solution
The compatible Java 2 JRE is not installed.	The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-79. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-17 shows JRE compatibility with ONS 15454 software releases.

Table 1-17 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R2.2.1 and earlier	Yes	No	No
ONS 15454 R2.2.2	Yes	Yes	No
ONS 15454 R3.0	Yes	Yes	No
ONS 15454 R3.1	Yes	Yes	No
ONS 15454 R3.2	Yes	Yes	No
ONS 15454 R3.3	Yes	Yes	No
ONS 15454 R3.4	No	Yes	No
ONS 15454 R4.0[1]	No	Yes	No
ONS 15454 R4.1	No	Yes	No
ONS 15454 R4.5	No	Yes	No
ONS 15454 R4.6	No	Yes	Yes

[1] Software R4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.

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 in with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

Note After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 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.

1.8.9 Different CTC Releases Do Not Recognize Each Other

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

Table 1-18 describes the possible problem and the solution.

Table 1-18 Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the TCC2 card are incompatible.	This occurs when the TCC2 software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. **Note** Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-80.

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 downloads the JAR file from CTC.

Note After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 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.

1.8.10 Username or Password Do Not Match

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

Table 1-19 describes the possible problem and the solution.

Table 1-19 Username or Password Do Not Match

Possible Problem	Solution
The username or password entered does not match the information stored in the TCC2.	All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, type the CISCO15 user name in capital letters and click **Login** (no password is required). If you are using a CTC Software R2.2.2 or earlier and CISCO15 does not work, type cerent454 for the user name. Complete the "Verify Correct Username and Password" procedure on page 1-81.

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 (1 800 553-2447) to have them enter your system and create a new user name and password.

1.8.11 No IP Connectivity Exists Between Nodes

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

Table 1-20 describes the possible problem and the solution.

Table 1-20 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 "1.8.15 Ethernet Connections" section on page 1-83.

1.8.12 DCC Connection Lost

Symptom The node is usually accompanied by alarms and the nodes in the network view have a gray icon. This symptom is usually accompanied by an EOC alarm.

Table 1-21 describes the possible problem and the solution.

Table 1-21 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" alarm.

1.8.13 "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 1-22 describes the possible problem and the solution.

Table 1-22 "Path in Use" Error When Creating a Circuit

Possible Problem	Solution
Another user has already selected the same source port to create another circuit.	CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. Cancel the circuit creation and start over, or click **Back** until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.

1.8.14 Calculate and Design IP Subnets

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

Table 1-23 describes the possible problem and the solution.

Table 1-23 Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.	Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 IP capability, refer to the *Cisco ONS 15454 Reference Manual.*

1.8.15 Ethernet Connections

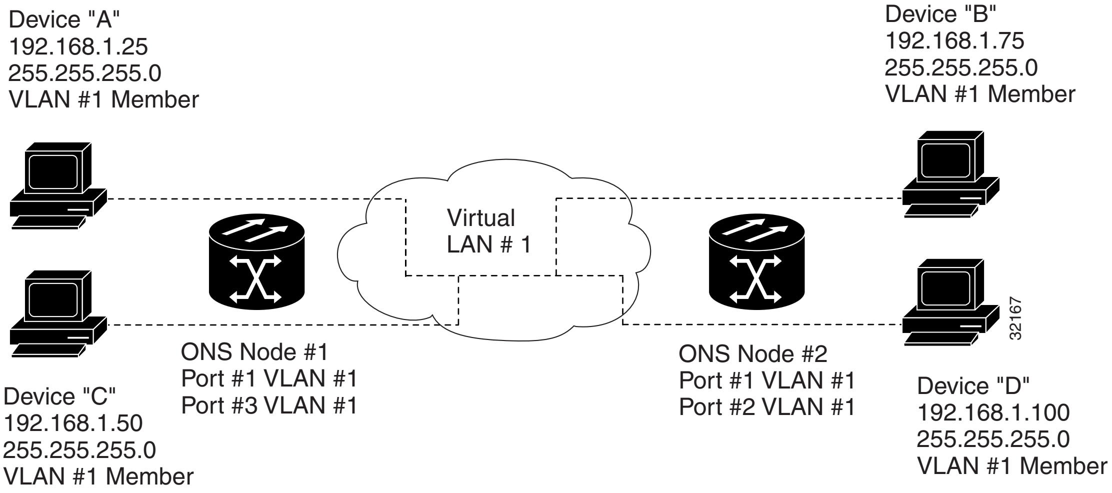
Symptom Ethernet connections appear to be broken or are not working properly.

Table 1-24 describes the possible problem and the solution.

Table 1-24 Calculate and Design IP Subnets

Possible Problem	Solution
Improperly seated connections.	You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-31 when using the steps in the "Verify Ethernet Connections" procedure on page 1-84.
Incorrect connections.	

Figure 1-31 Ethernet Connectivity Reference



Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET and dense wavelength division multiplexing (DWDM) 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 3 Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 2, "Alarm Troubleshooting."

Step 4 Verify that the ACT LED on the Ethernet card is green.

Step 5 Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.

Step 6 If no green link-integrity LED is illuminated for any of these ports:

a. Verify physical connectivity between the ONS 15454s and the attached device.

b. Verify that the ports are enabled on the Ethernet cards.

c. Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

d. Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.

e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the "Verify Card LED Operation" procedure on page 1-105.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices. Complete the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-70. If the ping is unsuccessful:

a. Verify that device A and device C are on the same IP subnet.

b. open the Ethernet card in CTC card view and click the **Provisioning > VLAN** 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 8 Repeat Step 7 for devices B and D.

Step 9 Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

1.8.16 VLAN Cannot Connect to Network Device from Untag Port

Symptom Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-32). They might also see a higher than normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Figure 1-32 VLAN with Ethernet Ports at Tagged and Untag

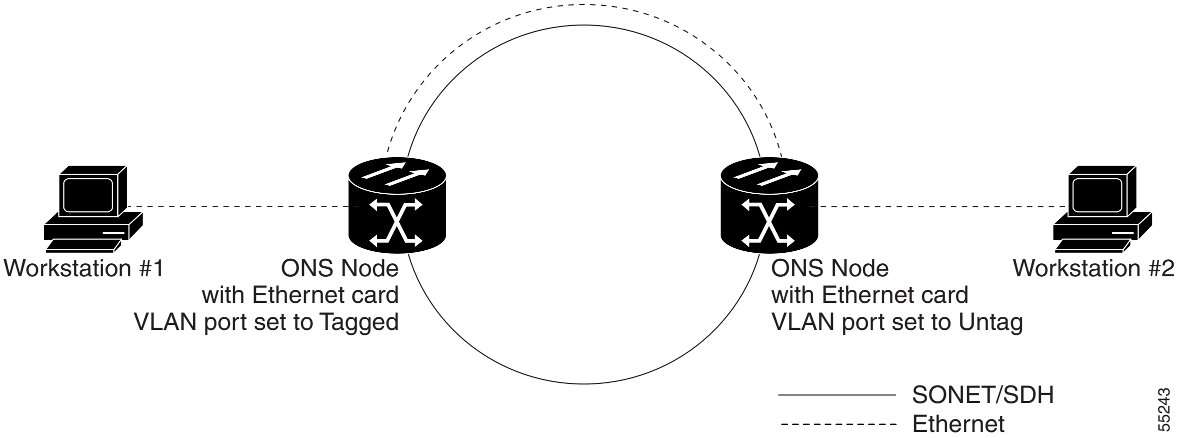


Table 1-25 describes the possible problems and the solution.

Table 1-25 Verify VLAN Connection to Network Device from Untag Port

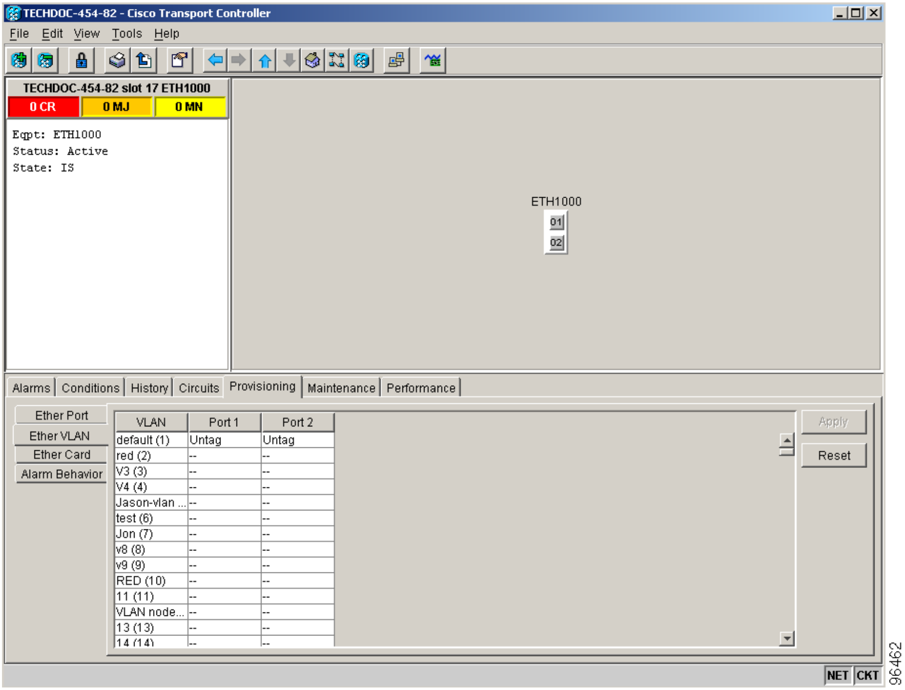
Possible Problem	Solution
The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet. Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.	The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non-IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance.

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 > Ether VLAN** tabs (Figure 1-33).

Figure 1-33 Configuring VLAN Membership for Individual Ethernet Ports



Eqpt: ETH1000
Status: Active
State: IS

VLAN	Port 1	Port 2
default (1)	Untag	Untag
red (2)	--	--
V3 (3)	--	--
V4 (4)	--	--
Jason-vlan ...	--	--
test (6)	--	--
Jon (7)	--	--
v8 (8)	--	--
v9 (9)	--	--
RED (10)	--	--
11 (11)	--	--
VLAN node...	--	--
13 (13)	--	--
14 (14)	--	--

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**.

1.8.17 Cross-Connect Card Oscillator Fails

Symptom: The XC or XCVT card can be affected by this problem. (In R4.6, the XC10G card automatically detects it.) 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 1-26 describes the potential cause(s) of the symptom and the solution(s).

Table 1-26 Cross-Connect Card Oscillator Fails

Possible Problem	Solution
The XC or XCVT card has oscillator failure.	1. If the Slot 8 cross-connect card is active, see the "1.8.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active" section on page 1-87. 2. If the Slot 10 cross-connect card is active, see the "1.8.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active" section on page 1-87.

1.8.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active

Step 1 If the CTNEQPT-PBPROT condition is reported against all I/O cards in the node and the Slot 8 cross-connect card is active, right-click the Slot 10 cross-connect card.

Step 2 Choose **Reset Card,** then click **OK**. (Slot 8 remains active and Slot 10 remains standby.)

Step 3 If the alarm remains, reseat the Slot 10 card.

Step 4 If CTNEQPT-PBPROT does not clear, replace the Slot 10 cross-connect card with a spare card.

Step 5 If CTNEQPT-PBPROT does not clear, replace the spare card placed in Slot 10 with the original cross-connect card.

Step 6 Right-click the Slot 8 card and choose **Reset Card**.

Step 7 Click **OK** to activate the Slot 10 card and place the Slot 8 card in standby.

Step 8 If you then see the CTNEQPT-PBWORK condition raised against all I/O cards in the node, verify that CTNEQPT-PBPROT has cleared on all I/O cards. Seeing CTNEQPT-PBWORK on the cards indicates that Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. Otherwise, go toStep 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.

1.8.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active

Step 1 If the CTNEQPT-PBWORK condition is reported against all I/O cards in the node and the Slot 10 card is active, right-click the Slot 8 cross-connect card.

Step 2 Choose **Reset Card** and click **OK**. (Slot 10 remains active and Slot 8 remains standby.)

Step 3 If the CTNEQPT-PBWORK condition does not clear, reseat the Slot 8 cross-connect card.

Step 4 If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.

Step 5 If the condition does not clear, replace the spare card placed in Slot 8 with the original cross-connect card.

Step 6 Right-click the Slot 10 cross-connect card.

Step 7 Choose **Reset Card** and click **OK**. The Slot 8 cross-connect card becomes active and Slot 10 becomes standby.

Step 8 If you have switched the Slot 8 card to active and continue to see CTNEQPT-PBWORK reported against all I/O cards in the node, this indicates the Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. If not, go to Step 9.

a. Replace the Slot 8 cross-connect card with a spare card. (The Slot 10 card is made active.)

b. Reseat the Slot 10 cross-connect card to make Slot 8 active.

c. Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

Step 9 If you then see the CTNEQPT-PBPROT condition raised against all I/O cards, verify that CTNEQPT-PBWORK has cleared on the I/O cards. This indicates that Slot 10 has a bad oscillator. If so, complete the following substeps:

a. Replace the Slot 10 cross-connect card with a spare card. (Slot 10 remains standby.)

b. Reseat the Slot 8 cross-connect card to activate the Slot 10 card and make Slot 8 standby.

c. Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

1.9 Circuits and Timing

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

1.9.1 OC-N Circuit Transitions to Partial State

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

- OOS_PARTIAL: At least one of the OC-N 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 OC-N 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 OC-N circuit is in the OOS_AINS state and at least one other connection in the circuit is in IS or OOS_AINS state.

Table 1-27 describes the possible problems and the solutions.

Table 1-27 Circuit in Partial State

Possible Problem	Solution
During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.	Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-89. Log into the circuit node that did not change to the desired state and determine the version of software. If the software on the node is Software R3.3 or earlier, upgrade the software. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. **Note** If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by using only the circuit state supported in the earlier software version.
During an automatic transition, some path-level defects and/or alarms were detected on the circuit.	Determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-89. Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.
One end of the circuit is not properly terminated.	

View the State of OC-N Circuit Nodes

Note This procedure does not apply to Software R4.6 DWDM cards.

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the *_PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab (if you are viewing a SONET circuit).

The State tab window lists the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

1.9.2 AIS-V on DS3XM-6 Unused VT Circuits

Symptom An incomplete circuit path causes an AIS.

Table 1-28 describes the possible problem and the solution.

Table 1-28 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. Complete the "Clear AIS-V on DS3XM-6 Unused VT Circuits" procedure on page 1-90.

Clear AIS-V on DS3XM-6 Unused VT Circuits

Note This procedure does not apply to Software R4.6 DWDM cards or ML-Series cards.

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, or VT number.

Step 3 Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

Step 4 Uncheck the bidirectional check box in the circuit creation window.

Step 5 Give the unidirectional VT circuit an easily recognizable name, such as "delete me."

Step 6 Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** 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 dialog 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 **Alarms** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the DS3XM-6 cards.

1.9.3 Circuit Creation Error with VT1.5 Circuit

Symptom You receive an "Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at *node_name*" message when trying to create a VT1.5 circuit in CTC.

Table 1-29 describes the possible problem and the solution.

Table 1-29 Circuit Creation Error with VT1.5 Circuit

Possible Problem	Solution
You might 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 exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a path protection or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Guide* for more information.

1.9.4 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 1-30 describes the possible problem and the solution.

Table 1-30 Unable to Create Circuit from DS-3 Card to DS3XM-6 Card

Possible Problem	Solution
A DS-3 card and a DS3XM-6 card have different functions.	A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. Thus, you can create a circuit from a DS3XM-6 card to a DS-1 card, but not from a DS3XM-6 card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 has a VT payload with a C2 hex value of 02. **Note** You can find instructions for creating circuits in the *Cisco ONS 15454 Procedure Guide*.

1.9.5 DS-3 Card Does Not Report AIS-P From External Equipment

Symptom A DS3-12, DS3N-12, DS3-12E, or DS3N-12E card does not report STS AIS-P from the external equipment/line side.

Table 1-31 on page 1-91 describes the possible problem and the solution.

Table 1-31 DS3 Card Does Not Report AIS-P From External Equipment

Possible Problem	Solution
The card is functioning as designed.	This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. DS3-12, DS3N-12, DS3-12E, and 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 about the PM capabilities of the DS3-12, DS3N-12, DS3-12E or DS3N-12E cards, refer to the *Cisco ONS 15454 Reference Manual*.

1.9.6 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Table 1-32 describes the possible problem and the solution.

Table 1-32 OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the ONS 15454.	For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Procedure Guide*.

1.9.7 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Table 1-33 describes the possible problems and the solution.

Table 1-33 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 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of ± 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x 10^{-7}/day, including temperature. ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.
The optical or building integrated timing supply (BITS) input is not functioning.	
The synchronization status messaging (SSM) message is set to do not use for synchronization (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.	

1.9.8 Holdover Synchronization Alarm

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

Table 1-34 describes the possible problem and the solution.

Table 1-34 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 "2.7.128 HLDOVRSYNC" section on page 2-104 for a detailed description of this alarm. **Note** The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

1.9.9 Free-Running Synchronization Mode

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

Table 1-35 describes the possible problem and the solution.

Table 1-35 Free-Running Synchronization Mode

Possible Problem	Solution
No reliable reference input is available.	The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" condition on page 2-96 for a detailed description.

1.9.10 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy chain the BITS sources.

Table 1-36 describes the possible problem and the solution.

Table 1-36 Daisy-Chained BITS Sources Not Functioning

Possible Problem	Solution
Daisy-chained BITS sources are not supported on the ONS 15454.	Daisy-chained BITS sources cause additional wander buildup in the network and are therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

1.9.11 Blinking STAT LED after Installing a Card

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

Table 1-37 describes the possible problem and the solution.

Table 1-37 Blinking STAT LED on Installed Card

Possible Problem	Solution
The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.	The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an "EQPT" alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Physically Replace a Card" procedure on page 2-219. ⚠ **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.

1.10 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.

1.10.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Table 1-38 describes the possible problem and the solution.

Table 1-38 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 "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using the "1.10.2 Faulty Fiber-Optic Connections" section on page 1-95.

1.10.2 Faulty Fiber-Optic Connections

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

Table 1-39 describes the possible problems and the solutions.

Table 1-39 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections.	Faulty fiber-optic connections can be the source of SONET/DWDM alarms and signal errors. Complete the "Verify Fiber-Optic Connections" procedure on page 1-95.
Faulty CAT-5 cables.	Faulty CAT-5 cables can be the source of SONET/DWDM alarms and signal errors. Complete the "1.10.2.1 Crimp Replacement LAN Cables" section on page 1-97.
Faulty Gigabit Interface Converters (GBIC).	Faulty GBICs can be the source of SONET/DWDM alarms and signal errors. See the "1.10.2.2 Replace Faulty GBIC or SFP Connectors" section on page 1-98.

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.**

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.

> **Note** SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

- **a.** Remove the Rx end of the suspect fiber.
- **b.** Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.
- **c.** Determine the power level of fiber with the fiber-optic power meter.
- **d.** Verify the power meter is set to the appropriate wavelength for the OC-N card being tested (either 1310 nm or 1550 nm depending on the specific card).
- **e.** Verify that the power level falls within the range specified for the card if it is an OC-N card; see the "1.10.3 OC-N Card Transmit and Receive Levels" section on page 1-102.

Step 4 If the power level falls below the specified range for the OC-N card:

a. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

b. Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.

IR cards transmit a lower output power than LR cards.

d. Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

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

e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

- Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
- Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
- Excessive number of fiber splices; splices take approximately 0.5 dB each.

Note These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the OC-N card failed.

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

b. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the OC-N card.

⚠ **Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. 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 LR card is not being used when an ONS IR card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter 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.

1.10.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-34 shows the wiring of an RJ-45 connector. Figure 1-35 shows a LAN cable layout, and Table 1-40 shows the cable pinouts. Figure 1-36 shows a cross-over cable layout, and Table 1-41 shows the cross-over pinouts.

Figure 1-34 RJ-45 Pin Numbers

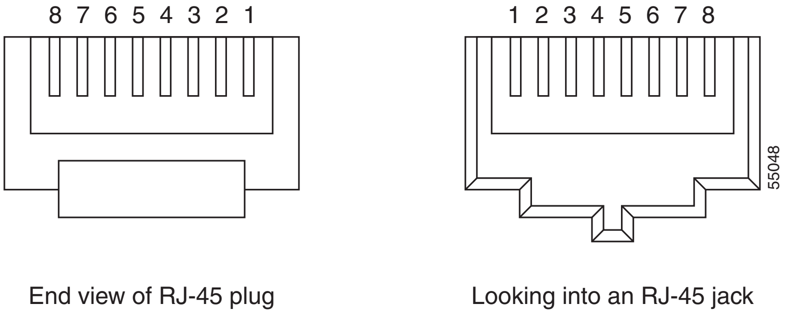


Figure 1-35 LAN Cable Layout

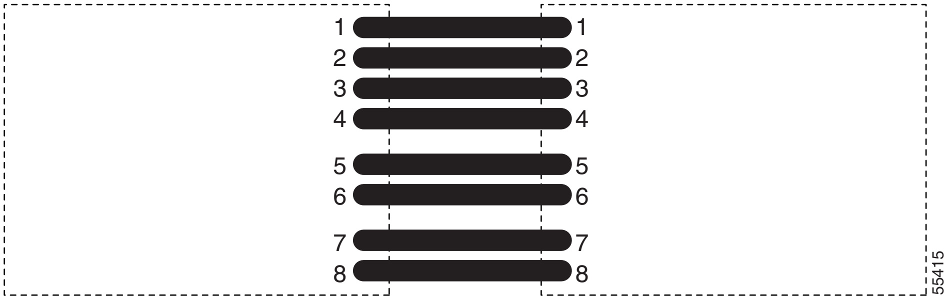


Table 1-40 LAN Cable Pinout

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 1-36 Cross-Over Cable Layout

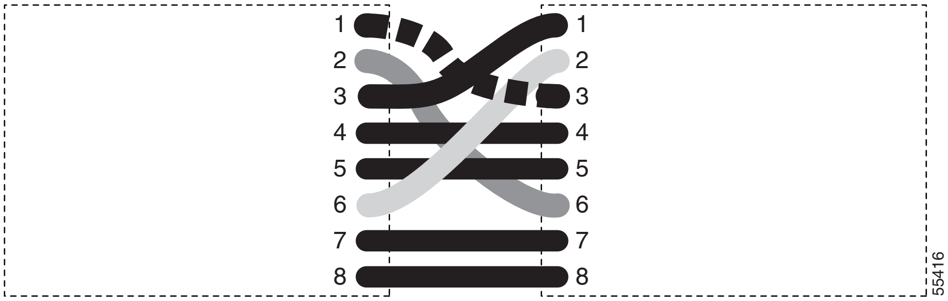


Table 1-41 Cross-Over Cable Pinout

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.

1.10.2.2 Replace Faulty GBIC or SFP Connectors

GBICs and small form-factor pluggables (SFP) are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning **GBICs are Class I laser products. These products have been tested and comply with Class I limits.**

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

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities, see Table 1-42 and Table 1-43 on page 1-100, and refer to the *Cisco ONS 15454 Reference Guide*.

Note GBICs and SFPs must be matched on either end by type: SX to SX, LX to LX, or ZX to ZX.

Note DWDM and coarse wavelength division multiplexing (CWDM) GBICs do not function with Software R4.6.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G-Series, or G1K-4 card. The other model has a locking handle. Both models are shown in Figure 1-37.

Figure 1-37 GBICs

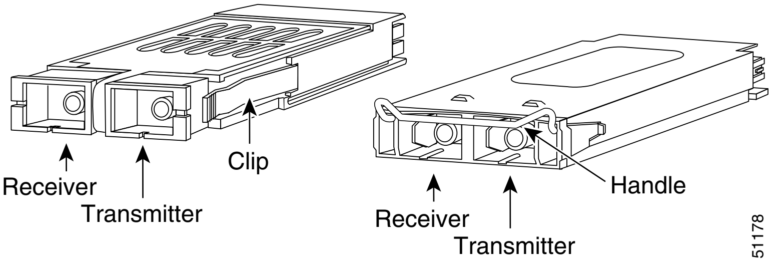


Table 1-42 shows the available GBICs. Table 1-43 shows the available SFPs.

Note GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Table 1-42 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G-Series G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=

Table 1-42 Available GBICs (continued)

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseLX	E1000-2-G G-Series G1K-4	Long reach	Single-mode fiber up to 10 km long	15454E-GBIC-LX=
1000BaseZX	G-Series G1K-4	Extra long reach	Single-mode fiber up to 70 km long	15454E-GBIC-ZX=

Table 1-43 Available SFPs

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	ML1000-2	Short reach	Multimode fiber up to 550 m long	15454E-SFP-LC-SX=
1000BaseLX	ML1000-2	Long reach	Single-mode fiber up to 10 km long	15454E-SFP-LC-LX=

Remove GBIC or SFP Connectors

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector.

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

Step 2 Release the GBIC or SFP from the slot by simultaneously squeezing the two plastic tabs on each side.

Step 3 Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Installing a GBIC with Clips

Step 1 Remove the GBIC from its protective packaging.

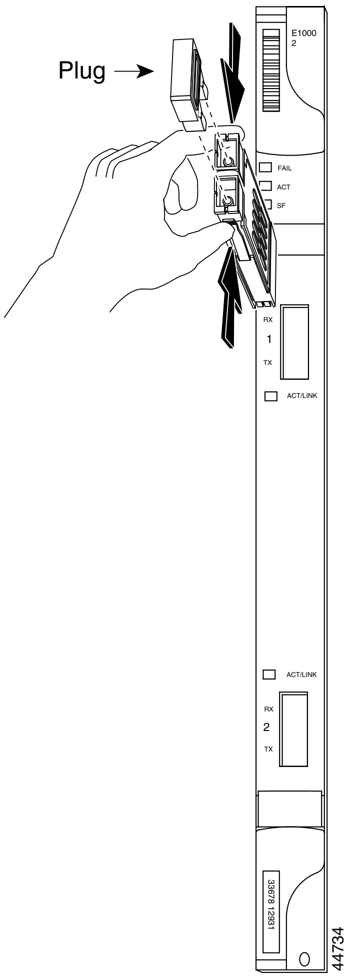
Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G-Series card (Figure 1-38).

Note GBICs are keyed to prevent incorrect installation.

Figure 1-38 GBIC Installation (with Clips)



Step 5 Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

Step 7 Return to your originating procedure (NTP).

Installing a GBIC with a Handle

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Remove the protective plug from the SC-type connector.

Step 5 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, G1K-4, or G-Series card.

Note GBICs are keyed to prevent incorrect installation.

Step 6 Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.

Step 7 Return to your originating procedure (NTP).

1.10.3 OC-N Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate. Table 1-44 lists these levels.

Table 1-44 OC-N Card Transmit and Receive Levels

OC-N Card	Receive	Transmit
OC3 IR4/STM1SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC3 IR/STM 1SH 1310-8	–30 to –8 dBm	–15 to –8 dBm
OC12 IR/STM4 SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC12 LR/STM4 LH 1310	–28 to –8 dBm	–3 to +2 dBm
OC12 LR/STM4 LH 1550	–28 to –8 dBm	–3 to +2 dBm
OC12 IR/STM4 SH 1310-4	–28 to –8 dBm	–3 to +2 dBm
OC48 IR/STM16 SH AS 1310	–18 to 0 dBm	–5 to 0 dBm
OC48 LR/STM16 LH AS 1550	–28 to –8 dBm	–2 to +3 dBm
OC48 ELR/STM16 EH 100GHz	–28 to –8 dBm	–2 to 0 dBm
OC192 SR/STM64 IO 1310	–11 to –1 dBm	–6 to –1 dBm
OC192 IR STM64 SH 1550	–14 to –1 dBm	–1 to +2 dBm
OC192 LR/STM64 LH 1550	–21 to –9 dBm	+7 to +10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	–22 to –9 dBm	+3 to +6 dBm
TXP-MR-10G Trunk side: Client side:	 –26 to –8 dBm –14 to –1 dBm	 –16 to +3 dBm –6 to –1 dBm
MXP-2.5G-10G Trunk side: Client side:	 –26 to –8 dBm depends on SFP	 –16 to +3 dBm depends on SFP

1.11 Power and LED Tests

This section provides symptoms and solutions for power supply, power consumption, and LED indicator problems.

1.11.1 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 1-45 describes the possible problems and the solution.

Table 1-45 Power Supply Problems

Possible Problem	Solution
Loss of power or low voltage. Improperly connected power supply.	The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tabs and change the Date and Time fields. Complete the "Isolate the Cause of Power Supply Problems" procedure on page 1-103.

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.**

Caution Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15454 show signs of fluctuating power or power loss:

a. Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.

b. Verify that the power cable is #12 or #14 AWG and in good condition.

c. Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.

d. Verify that 20-A fuses are used in the fuse panel.

e. Verify that the fuses are not blown.

f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.

g. Verify that the DC power source has enough capacity to carry the power load.

h. If the DC power source is battery-based:

- Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.
- Check the age of the batteries. Battery performance decreases with age.
- Check for opens and shorts in batteries, which might affect power output.
- If brownouts occur, the power load and fuses might be too high for the battery plant.

Step 2 If multiple pieces of site equipment show signs of fluctuating power or power loss:

a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer’s documentation for specific instructions.

b. Check for excessive power drains caused by other equipment, such as generators.

c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

1.11.2 Power Consumption for Node and Cards

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

Table 1-46 describes the possible problem and the solution.

Table 1-46 Power Consumption for Node and Cards

Possible Problem	Solution
Improper power supply.	Refer to power information in the *Cisco ONS 15454 Reference Guide*.

1.11.3 Lamp Tests for Card LEDs

The LED lamp test determines whether card-level LEDs are operational. For optical and electrical cards, this test also causes port-level LEDs to illuminate. For all other data cards, only card-level LEDs light. For these cards, port-level LEDs can be compared to the given guidelines to determine whether they are working correctly.

Symptom Optical (OC-N) or electrical (DS-N) card LEDs do not light, or you are unsure whether the LEDs are working properly.

Optical and electrical port LEDs light during the lamp test. Other data card types only illuminate card-level LEDs during the test. Table 1-47 describes the possible problem and the solution for optical and electrical cards.

Table 1-47 Lamp Test for Optical and Electrical Card LEDs

Possible Problem	Solution
Faulty optical and electrical port LED	A lamp test verifies that all the port 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. Complete the "Verify Card LED Operation" procedure on page 1-105.

Verify Card LED Operation

Step 1 In CTC, click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate as previously noted for several seconds.

Step 4 Click **OK** on the Lamp Test Run dialog box.

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco TAC (1 800 553-2447).

Symptom G-Series Ethernet or FC_MR-4 card LED does not light, or you are unsure if LEDs are working properly.

Table 1-48 describes the possible problem and the solution for G-Series and FC_MR-4 cards.

Note G-Series and FC_MR-4 card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Table 1-48 Lamp Test for G-Series or FC_MR-4 Card LEDs

Possible Problem	Solution
Faulty LED	Complete the "Verify G-Series Ethernet or FC_MR-4 Card LED Operation" procedure on page 1-105.

Verify G-Series Ethernet or FC_MR-4 Card LED Operation

Step 1 Complete the "Verify Card LED Operation" procedure on page 1-105 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the G-Series Ethernet port LEDs are operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur if there is a loss of receive link (such as a disconnected link or unplugged GBIC). An LOS alarm could be present on the port.
- Amber port LED: Should only occur if a port is disabled but the link is connected; or if the port is enabled and the link is connected, but a transport failure is present. A TPTFAIL alarm can be present on the port.

- Green port LED: Should occur if the port is enabled and has no errors against it or traffic in it; can also occur if the port is enabled, has no errors, and is running traffic proportionate to the blink rate. No traffic-affecting port alarms should be present.

Step 3 If you are unable to determine the port state, contact Cisco TAC (1 800 553-2447).

Symptom E-Series or ML-Series Ethernet card LED does not light, or you are unsure if LEDs are working properly.

Table 1-48 describes the possible problem and the solution for E-Series and ML-Series Ethernet cards.

Note E-Series and ML-Series card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Table 1-49 Lamp Test for E-Series and ML-Series Ethernet Card LEDs

Possible Problem	Solution
Faulty LED	Complete the "Verify E-Series and ML-Series Ethernet Card LED Operation" procedure on page 1-106.

Verify E-Series and ML-Series Ethernet Card LED Operation

Step 1 Complete the "Verify Card LED Operation" procedure on page 1-105 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the single E-Series or ML-Series Ethernet port LED is operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur is there is a loss of receive link (such as a disconnected link or unplugged GBIC), or if traffic is flowing in one direction (either transmit or receive). A CARLOSS alarm could be present on the port.
- Amber port LED: Should only occur if the link is connected and the physical port is transmitting and receiving traffic.
- Green port LED: Should occur if the link is up and no traffic is flowing on the port.

Step 3 If you are unable to determine the port state, contact Cisco TAC (1 800 553-2447).

CHAPTER 2

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-4 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-6 provides a list of alarms organized alphabetically. Table 2-8 on page 2-11 provides a list of alarms organized by alarm type. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

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

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

For alarm profile information, refer to the *Cisco ONS 15454 Procedure Guide*.

2.1 Alarm Index by Default Severity

The following tables group alarms and conditions by the severity displayed in the CTC Alarms window in the severity (SEV) column, which is the same severity used when reported by TL1. All severities listed in this manual are the default profile settings. Alarm severities can be altered from default settings for individual alarms or groups of alarms by creating a nondefault alarm profile and applying it on a port, card, or shelf basis. All settings (default or user-defined) that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

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 lists Critical alarms.

Table 2-1 Critical Alarm Index

AUTOLSROFF, page 2-35	LOF (DS3), page 2-122	MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151
BKUPMEMP, page 2-42	LOF (EC1-12), page 2-123	OPWR-HFAIL, page 2-160
CKTDOWN, page 2-51	LOF (OCN), page 2-123	OPWR-LFAIL, page 2-161
COMIOXC, page 2-54	LOF (TRUNK), page 2-124	OTUK-LOF, page 2-162
CTNEQPT-PBPROT, page 2-59	LOM, page 2-124 for STSTRM, TRUNK	PLM-P, page 2-167
CTNEQPT-PBWORK, page 2-61	LOP-P, page 2-125 for STSMON, STSTRM	PORT-CODE-MISM, page 2-168
EQPT, page 2-69	LOS (CLIENT), page 2-127	PORT-COMM-FAIL, page 2-168
EQPT-MISS, page 2-70	LOS (DS3), page 2-129	PORT-MISMATCH, page 2-169 (for CLIENT only)
FAN, page 2-83	LOS (EC1-12), page 2-130	PORT-MISSING, page 2-169
GAIN-HFAIL, page 2-98	LOS (OCN), page 2-132	SQM, page 2-188 for STSTRM
GAIN-LFAIL, page 2-99	LOS (OTS), page 2-134	SWMTXMOD, page 2-193
GE-OOSYNC, page 2-100	LOS (TRUNK), page 2-135	TIM, page 2-198 (for CLIENT, TRUNK only)
HITEMP, page 2-103 (for NE only)	LOS-P, page 2-136	TIM-P, page 2-199, for STSTRM
I-HITEMP, page 2-105	MEA (AIP), page 2-148	UNEQ-P, page 2-204
IMPROPRMVL, page 2-105	MEA (EQPT), page 2-148	VOA-HFAIL, page 2-208
LOA, page 2-119	MEA (FAN), page 2-150	VOA-LFAIL, page 2-209
LOF (CLIENT), page 2-121	—	—

2.1.2 Major Alarms (MJ)

Table 2-2 lists Major alarms.

Table 2-2 Major Alarm Index

APC-DISABLED, page 2-24	DUP-IPADDR, page 2-65	LOS (BITS), page 2-127
APC-FAIL, page 2-25	DUP-NODENAME, page 2-65	LOS (DS1), page 2-128
APSCM, page 2-29	EHIBATVG, page 2-66	LWBATVG, page 2-145
APSCNMIS, page 2-30	ELWBATVG, page 2-66	MEM-GONE, page 2-151
AWG-FAIL, page 2-40	EOC, page 2-66	OPTNTWMIS, page 2-157
AWG-OVERTEMP, page 2-41	EOC-L, page 2-68	PEER-NORESPONSE, page 2-166
BAT-FAIL, page 2-41	E-W-MISMATCH, page 2-73	PLM-V, page 2-167
BLSROSYNC, page 2-43	EXTRA-TRAF-PREEMPT, page 2-77	PRC-DUPID, page 2-170

Table 2-2 Major Alarm Index (continued)

CARLOSS (CLIENT), page 2-43	FANDEGRADE, page 2-84	RCVR-MISS, page 2-173
CARLOSS (EQPT), page 2-44	FEC-MISM, page 2-84	RING-ID-MIS, page 2-176
CARLOSS (E100T, E1000F), page 2-45	GCC-EOC, page 2-100	RING-MISMATCH, page 2-176
CARLOSS (G1000), page 2-46	HIBATVG, page 2-100	SQM, page 2-188 for VT-TERM
CARLOSS (ML100T, ML1000), page 2-49	HLDOVRSYNC, page 2-104	SYSBOOT, page 2-197
CARLOSS (TRUNK), page 2-50	INC-SIGLOSS, page 2-109	TPTFAIL (FC_MR-4), page 2-200
CONTBUS-A-18, page 2-55	INC-SYNCLOSS, page 2-110	TPTFAIL (G1000), page 2-200
CONTBUS-B-18, page 2-55	INVMACADR, page 2-111	TPTFAIL (ML100T, ML1000), page 2-201
CONTBUS-IO-A, page 2-56	LOF (BITS), page 2-120	TRMT, page 2-201
CONTBUS-IO-B, page 2-57	LOF (DS1), page 2-121	TRMT-MISS, page 2-202
DBOSYNC, page 2-62	LOM, page 2-124 for VT-TERM	UNEQ-V, page 2-206
DSP-COMM-FAIL, page 2-63	LOP-V, page 2-125	WVL-MISMATCH, page 2-210
DSP-FAIL, page 2-63	—	—

2.1.3 Minor Alarms (MN)

Table 2-3 lists Minor alarms.

Table 2-3 Minor Alarm Index

APSB, page 2-26	GAIN-LDEG, page 2-98	OPWR-LDEG, page 2-160
APSCDFLTK, page 2-27	HI-LASERBIAS, page 2-101	PROTNA, page 2-170
APSC-IMP, page 2-28	HI-RXPOWER, page 2-102	PTIM, page 2-171
APSCINCON, page 2-29	HITEMP, page 2-103	PWR-REDUN, page 2-172
APSMM, page 2-32	HI-TXPOWER, page 2-103	RSVP-HELLODOWN, page 2-177
AUTORESET, page 2-36	KBYTE-APS-CHANNEL-FAILURE, page 2-114	SFTWDOWN, page 2-183
AUTOSW-LOP (VT-MON), page 2-37	LASERBIAS-DEG, page 2-115	SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
AUTOSW-UNEQ (VT-MON), page 2-39	LASEREOL, page 2-116	SH-INS-LOSS-VAR-DEG-LOW, page 2-184
AWG-DEG, page 2-40	LASERTEMP-DEG, page 2-117	SNTP-HOST, page 2-185
CASETEMP-DEG, page 2-50	LMP-HELLODOWN, page 2-118	SSM-FAIL, page 2-189
COMM-FAIL, page 2-54	LMP-NDFAIL, page 2-118	SYNCPRI, page 2-195
DATAFLT, page 2-62	LO-RXPOWER, page 2-126	SYNCSEC, page 2-196
ERROR-CONFIG, page 2-72	LOS (FUDC), page 2-131	SYNCTHIRD, page 2-197
EXCCOL, page 2-75	LO-TXPOWER, page 2-137	TIM-MON, page 2-198
EXT, page 2-77	MEM-LOW, page 2-151	TIM-P, page 2-199, for STSMON

Table 2-3 Minor Alarm Index (continued)

FEPRLF, page 2-93	NOT-AUTHENTICATED, page 2-153	VOA-HDEG, page 2-207
FSTSYNC, page 2-97	OPTNTWMIS, page 2-157	VOA-LDEG, page 2-208
GAIN-HDEG, page 2-97	OPWR-HDEG, page 2-158	—

2.1.4 NA Conditions

Table 2-4 lists not alarmed (NA) conditions.

Table 2-4 NA Conditions Index

ALS, page 2-23	FRNGSYNC, page 2-96	OTUK-TIM, page 2-164
AMPLI-INIT, page 2-24	FULLPASSTHR-BI, page 2-97	OUT-OF-SYNC, page 2-164
APSIMP, page 2-31	INC-GFP-OUTOFFRAME, page 2-107	PDI-P, page 2-164
AS-CMD, page 2-32	INC-GFP-SIGLOSS, page 2-108	PORT-MISMATCH, page 2-169 for FC_MR-4
AS-MT, page 2-33	INC-GFP-SYNCLOSS, page 2-108	RAI, page 2-172
AUD-LOG-LOSS, page 2-34	INC-ISD, page 2-109	RING-SW-EAST, page 2-177
AUD-LOG-LOW, page 2-34	INHSWPR, page 2-110	RING-SW-WEST, page 2-177
AUTOSW-LOP (STSMON), page 2-37	INHSWWKG, page 2-110	RUNCFG-SAVENEED, page 2-178
AUTOSW-PDI, page 2-38	INTRUSION-PSWD, page 2-111	SD (CLIENT, TRUNK), page 2-178
AUTOSW-SDBER, page 2-38	IOSCFGCOPY, page 2-113	SD (DS1, DS3), page 2-178
AUTOSW-SFBER, page 2-38	KB-PASSTHR, page 2-114	SD-L, page 2-180
AUTOSW-UNEQ (STSMON), page 2-39	LAN-POL-REV, page 2-114	SD-P, page 2-180
AWG-WARM-UP, page 2-41	LASER-APR, page 2-115	SF (CLIENT, TRUNK), page 2-181
CLDRESTART, page 2-53	LASERBIAS-FAIL, page 2-116	SF (DS1, DS3), page 2-182
CTNEQPT-MISMATCH, page 2-58	LASEREOL, page 2-116	SF-L, page 2-182
DS3-MISM, page 2-64	LKOUTPR-S, page 2-118	SF-P, page 2-183
ETH-LINKLOSS, page 2-73	LOCKOUT-REQ, page 2-119	SHUTTER-OPEN, page 2-184
EXERCISE-RING-FAIL, page 2-76	LPBKCRS, page 2-138	SPAN-SW-EAST, page 2-185
EXERCISE-SPAN-FAIL, page 2-76	LPBKDS1FEAC, page 2-139	SPAN-SW-WEST, page 2-186
FAILTOSW, page 2-78	LPBKDS1FEAC-CMD, page 2-139	SQUELCH, page 2-186
FAILTOSW-PATH, page 2-79	LPBKDS3FEAC, page 2-139	SQUELCHED, page 2-187
FAILTOSWR, page 2-79	LPBKDS3FEAC-CMD, page 2-140	SSM-DUS, page 2-188
FAILTOSWS, page 2-81	LPBKFACILITY (CLIENT, TRUNK), page 2-140	SSM-LNC, page 2-189
FE-AIS, page 2-84	LPBKFACILITY (DS1, DS3), page 2-141	SSM-OFF, page 2-189

Table 2-4 NA Conditions Index (continued)

FE-DS1-MULTLOS, page 2-85	LPBKFACILITY (EC1-12), page 2-141	SSM-PRC, page 2-190
FE-DS1-NSA, page 2-85	LPBKFACILITY (G1000), page 2-142	SSM-PRS, page 2-190
FE-DS1-SA, page 2-86	LPBKFACILITY (OCN), page 2-142	SSM-RES, page 2-190
FE-DS1-SNGLLOS, page 2-86	LPBKTERMINAL (CLIENT, TRUNK), page 2-143	SSM-SMC, page 2-191
FE-DS3-NSA, page 2-87	LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	SSM-STU, page 2-191
FE-DS3-SA, page 2-88	LPBKTERMINAL (G1000), page 2-144	SSM-ST2, page 2-191
FE-EQPT-NSA, page 2-88	MAN-REQ, page 2-145	SSM-ST3, page 2-192
FE-FRCDWKSWPR-RING, page 2-89	MANRESET, page 2-146	SSM-ST3E, page 2-192
FE-FRCDWKSWPR-SPAN, page 2-89	MANSWTOINT, page 2-146	SSM-ST4, page 2-192
FE-IDLE, page 2-90	MANSWTOPRI, page 2-146	SSM-TNC, page 2-192
FE-LOCKOUTOFPR-SPAN, page 2-90	MANSWTOSEC, page 2-146	SWTOPRI, page 2-194
FE-LOF, page 2-91	MANSWTOTHIRD, page 2-147	SWTOSEC, page 2-194
FE-LOS, page 2-91	MANUAL-REQ-RING, page 2-147	SWTOTHIRD, page 2-194
FE-MANWKSWPR-RING, page 2-92	MANUAL-REQ-SPAN, page 2-147	SYNC-FREQ, page 2-195
FE-MANWKSWPR-SPAN, page 2-92	NO-CONFIG, page 2-152	TIM, page 2-198 (for OCN only)
FORCED-REQ, page 2-94	ODUK-SD-PM, page 2-156	TX-RAI, page 2-203
FORCED-REQ-RING, page 2-94	ODUK-SF-PM, page 2-156	UNC-WORD, page 2-203
FORCED-REQ-SPAN, page 2-95	ODUK-TIM-PM, page 2-156	VCG-DEG, page 2-206
FRCDSWTOINT, page 2-95	OOU-TPT, page 2-157	VCG-DOWN, page 2-207
FRCDSWTOPRI, page 2-95	OTUK-SD, page 2-163	WKSWPR, page 2-209
FRCDSWTOSEC, page 2-96	OTUK-SF, page 2-163	WTR, page 2-210
FRCDSWTOTHIRD, page 2-96	—	—

2.1.5 NR Conditions

Table 2-5 lists not reported (NR) conditions.

Table 2-5 NR Conditions Index

AIS, page 2-21	ERFI-P-SRVR, page 2-71	OTUK-BDI, page 2-162
AIS-L, page 2-22	ODUK-AIS-PM, page 2-154	RFI, page 2-173
AIS-P, page 2-22	ODUK-BDI-PM, page 2-154	RFI-L, page 2-174
AIS-V, page 2-23	ODUK-LCK-PM, page 2-155	RFI-P, page 2-174
AUTOSW-AIS, page 2-36	ODUK-OCI-PM, page 2-155	RFI-V, page 2-175
ERFI-P-CONN, page 2-71	OTUK-AIS, page 2-161	TX-AIS, page 2-203
ERFI-P-PAYLD, page 2-71	—	—

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-6 lists alarms and conditions by the name displayed on the CTC Alarms window or Conditions window.

Table 2-6 Alphabetical Alarm Index

AIS, page 2-21	FRCDSWTOINT, page 2-95	ODUK-OCI-PM, page 2-155
AIS-L, page 2-22	FRCDSWTOPRI, page 2-95	ODUK-SD-PM, page 2-156
AIS-P, page 2-22	FRCDSWTOSEC, page 2-96	ODUK-SF-PM, page 2-156
AIS-V, page 2-23	FRCDSWTOTHIRD, page 2-96	ODUK-TIM-PM, page 2-156
ALS, page 2-23	FRNGSYNC, page 2-96	OOU-TPT, page 2-157
AMPLI-INIT, page 2-24	FSTSYNC, page 2-97	OPTNTWMIS, page 2-157
APC-DISABLED, page 2-24	FULLPASSTHR-BI, page 2-97	OPWR-HDEG, page 2-158
APC-FAIL, page 2-25	GAIN-HDEG, page 2-97	OPWR-HFAIL, page 2-160
APSB, page 2-26	GAIN-HFAIL, page 2-98	OPWR-LDEG, page 2-160
APSCDFLTK, page 2-27	GAIN-LDEG, page 2-98	OPWR-LFAIL, page 2-161
APSC-IMP, page 2-28	GAIN-LFAIL, page 2-99	OTUK-AIS, page 2-161
APSCINCON, page 2-29	GCC-EOC, page 2-100	OTUK-BDI, page 2-162
APSCM, page 2-29	GE-OOSYNC, page 2-100	OTUK-LOF, page 2-162
APSCNMIS, page 2-30	HIBATVG, page 2-100	OTUK-SD, page 2-163
APSIMP, page 2-31	HI-LASERBIAS, page 2-101	OTUK-SF, page 2-163
APSMM, page 2-32	HI-RXPOWER, page 2-102	OTUK-TIM, page 2-164
AS-CMD, page 2-32	HITEMP, page 2-103	OUT-OF-SYNC, page 2-164
AS-MT, page 2-33	HI-TXPOWER, page 2-103	PDI-P, page 2-164
AUD-LOG-LOSS, page 2-34	HLDOVRSYNC, page 2-104	PEER-NORESPONSE, page 2-166
AUD-LOG-LOW, page 2-34	I-HITEMP, page 2-105	PLM-P, page 2-167
AU-LOF, page 2-34	IMPROPRMVL, page 2-105	PLM-V, page 2-167
AUTOLSROFF, page 2-35	INC-GFP-OUTOFFRAME, page 2-107	PORT-CODE-MISM, page 2-168
AUTORESET, page 2-36	INC-GFP-SIGLOSS, page 2-108	PORT-COMM-FAIL, page 2-168
AUTOSW-AIS, page 2-36	INC-GFP-SYNCLOSS, page 2-108	PORT-MISMATCH, page 2-169
AUTOSW-LOP (STSMON), page 2-37	INC-ISD, page 2-109	PORT-MISSING, page 2-169
AUTOSW-LOP (VT-MON), page 2-37	INC-SIGLOSS, page 2-109	PRC-DUPID, page 2-170
AUTOSW-PDI, page 2-38	INC-SYNCLOSS, page 2-110	PROTNA, page 2-170
AUTOSW-SDBER, page 2-38	INC-ISD, page 2-109	PTIM, page 2-171
AUTOSW-SFBER, page 2-38	INHSWPR, page 2-110	PWR-REDUN, page 2-172
AUTOSW-UNEQ (STSMON), page 2-39	INHSWWKG, page 2-110	RAI, page 2-172
AUTOSW-UNEQ (VT-MON), page 2-39	INTRUSION-PSWD, page 2-111	RCVR-MISS, page 2-173
AWG-DEG, page 2-40	INVMACADR, page 2-111	RFI, page 2-173

Table 2-6 Alphabetical Alarm Index (continued)

AWG-FAIL, page 2-40	IOSCFGCOPY, page 2-113	RFI-L, page 2-174
AWG-OVERTEMP, page 2-41	KB-PASSTHR, page 2-114	RFI-P, page 2-174
AWG-WARM-UP, page 2-41	KBYTE-APS-CHANNEL-FAILURE, page 2-114	RFI-V, page 2-175
BAT-FAIL, page 2-41	LAN-POL-REV, page 2-114	RING-ID-MIS, page 2-176
BKUPMEMP, page 2-42	LASER-APR, page 2-115	RING-MISMATCH, page 2-176
BLSROSYNC, page 2-43	LASERBIAS-DEG, page 2-115	RING-SW-EAST, page 2-177
CARLOSS (CLIENT), page 2-43	LASERBIAS-FAIL, page 2-116	RING-SW-WEST, page 2-177
CARLOSS (EQPT), page 2-44	LASEREOL, page 2-116	RSVP-HELLODOWN, page 2-177
CARLOSS (E100T, E1000F), page 2-45	LASERTEMP-DEG, page 2-117	RUNCFG-SAVENEED, page 2-178
CARLOSS (G1000), page 2-46	LKOUTWK-S (NA), page 2-118	SD (CLIENT, TRUNK), page 2-178
CARLOSS (ML100T, ML1000), page 2-49	LKOUTPR-S, page 2-118	SD (DS1, DS3), page 2-178
CARLOSS (TRUNK), page 2-50	LMP-HELLODOWN, page 2-118	SD-L, page 2-180
CASETEMP-DEG, page 2-50	LMP-NDFAIL, page 2-118	SD-P, page 2-180
CKTDOWN, page 2-51	LOA, page 2-119	SF (CLIENT, TRUNK), page 2-181
CLDRESTART, page 2-53	LOCKOUT-REQ, page 2-119	SF (DS1, DS3), page 2-182
COMIOXC, page 2-54	LOF (BITS), page 2-120	SF-L, page 2-182
COMM-FAIL, page 2-54	LOF (CLIENT), page 2-121	SF-P, page 2-183
CONTBUS-A-18, page 2-55	LOF (DS1), page 2-121	SFTWDOWN, page 2-183
CONTBUS-B-18, page 2-55	LOF (DS3), page 2-122	SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
CONTBUS-IO-A, page 2-56	LOF (EC1-12), page 2-123	SH-INS-LOSS-VAR-DEG-LOW, page 2-184
CONTBUS-IO-B, page 2-57	LOF (OCN), page 2-123	SHUTTER-OPEN, page 2-184
CTNEQPT-MISMATCH, page 2-58	LOF (TRUNK), page 2-124	SNTP-HOST, page 2-185
CTNEQPT-PBPROT, page 2-59	LOM, page 2-124	SPAN-SW-EAST, page 2-185
CTNEQPT-PBWORK, page 2-61	LOP-P, page 2-125	SPAN-SW-WEST, page 2-186
DATAFLT, page 2-62	LOP-V, page 2-125	SQUELCH, page 2-186
DBOSYNC, page 2-62	LO-RXPOWER, page 2-126	SQUELCHED, page 2-187
DSP-COMM-FAIL, page 2-63	LO-TXPOWER, page 2-137	SQM, page 2-188
DSP-FAIL, page 2-63	LOS (BITS), page 2-127	SSM-DUS, page 2-188
DS3-MISM, page 2-64	LOS (CLIENT), page 2-127	SSM-FAIL, page 2-189
DUP-IPADDR, page 2-65	LOS (DS1), page 2-128	SSM-LNC, page 2-189
DUP-NODENAME, page 2-65	LOS (DS3), page 2-129	SSM-OFF, page 2-189
EHIBATVG, page 2-66	LOS (EC1-12), page 2-130	SSM-PRC, page 2-190
ELWBATVG, page 2-66	LOS (FUDC), page 2-131	SSM-PRS, page 2-190
EOC, page 2-66	LOS (OCN), page 2-132	SSM-RES, page 2-190
EOC-L, page 2-68	LOS (OTS), page 2-134	SSM-SDH-TN, page 2-190

Table 2-6 Alphabetical Alarm Index (continued)

EQPT, page 2-69	LOS (TRUNK), page 2-135	SSM-SETS, page 2-191
EQPT-MISS, page 2-70	LOS-P, page 2-136	SSM-SMC, page 2-191
ERFI-P-CONN, page 2-71	LPBKCRS, page 2-138	SSM-ST2, page 2-191
ERFI-P-PAYLD, page 2-71	LPBKDS1FEAC, page 2-139	SSM-ST3, page 2-192
ERFI-P-SRVR, page 2-71	LPBKDS1FEAC-CMD, page 2-139	SSM-ST3E, page 2-192
ERROR-CONFIG, page 2-72	LPBKDS3FEAC, page 2-139	SSM-ST4, page 2-192
ETH-LINKLOSS, page 2-73	LPBKDS3FEAC-CMD, page 2-140	SSM-STU, page 2-191
E-W-MISMATCH, page 2-73	LPBKFACILITY (DS1, DS3), page 2-141	SSM-TNC, page 2-192
EXCCOL, page 2-75	LPBKFACILITY (CLIENT, TRUNK), page 2-140	SWMTXMOD, page 2-193
EXERCISE-RING-FAIL, page 2-76	LPBKFACILITY (EC1-12), page 2-141	SWTOPRI, page 2-194
EXERCISE-SPAN-FAIL, page 2-76	LPBKFACILITY (G1000), page 2-142	SWTOSEC, page 2-194
EXT, page 2-77	LPBKFACILITY (OCN), page 2-142	SWTOTHIRD, page 2-194
EXTRA-TRAF-PREEMPT, page 2-77	LPBKTERMINAL (CLIENT, TRUNK), page 2-143	SYNC-FREQ, page 2-195
FAILTOSW, page 2-78	LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	SYNCPRI, page 2-195
FAILTOSW-PATH, page 2-79	LPBKTERMINAL (G1000), page 2-144	SYNCSEC, page 2-196
FAILTOSWR, page 2-79	LWBATVG, page 2-145	SYNCTHIRD, page 2-197
FAILTOSWS, page 2-81	MAN-REQ, page 2-145	SYSBOOT, page 2-197
FAN, page 2-83	MANRESET, page 2-146	TIM, page 2-198
FANDEGRADE, page 2-84	MANSWTOINT, page 2-146	TIM-MON, page 2-198
FE-AIS, page 2-84	MANSWTOPRI, page 2-146	TIM-P, page 2-199
FEC-MISM, page 2-84	MANSWTOSEC, page 2-146	TPTFAIL (FC_MR-4), page 2-200
FE-DS1-MULTLOS, page 2-85	MANSWTOTHIRD, page 2-147	TPTFAIL (G1000), page 2-200
FE-DS1-NSA, page 2-85	MANUAL-REQ-RING, page 2-147	TPTFAIL (ML100T, ML1000), page 2-201
FE-DS1-SA, page 2-86	MANUAL-REQ-SPAN, page 2-147	TRMT, page 2-201
FE-DS1-SNGLLOS, page 2-86	MEA (AIP), page 2-148	TRMT-MISS, page 2-202
FE-DS3-NSA, page 2-87	MEA (EQPT), page 2-148	TX-AIS, page 2-203
FE-DS3-SA, page 2-88	MEA (FAN), page 2-150	TX-RAI, page 2-203
FE-EQPT-NSA, page 2-88	MEM-GONE, page 2-151	UNC-WORD, page 2-203
FE-FRCDWKSWPR-RING, page 2-89	MEM-LOW, page 2-151	UNEQ-P, page 2-204
FE-FRCDWKSWPR-SPAN, page 2-89	MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	UNEQ-V, page 2-206
FE-IDLE, page 2-90	NO-CONFIG, page 2-152	VCG-DEG, page 2-206

Table 2-6 Alphabetical Alarm Index (continued)

FE-LOCKOUTOFPR-SPAN, page 2-90	NOT-AUTHENTICATED, page 2-153	VCG-DOWN, page 2-207
FE-LOF, page 2-91	NTWTPINC, page 2-153	VOA-HDEG, page 2-207
FE-LOS, page 2-91	OCHNC-ACTIV-FAIL, page 2-153	VOA-HFAIL, page 2-208
FE-MANWKSWPR-RING, page 2-92	OCHNC-DEACTIV-FAIL, page 2-153	VOA-LDEG, page 2-208
FE-MANWKSWPR-SPAN, page 2-92	OCHNC-FAIL, page 2-153	VOA-LFAIL, page 2-209
FEPRLF, page 2-93	OCHNC-INC, page 2-153	WKSWPR, page 2-209
FORCED-REQ, page 2-94	ODUK-AIS-PM, page 2-154	WTR, page 2-210
FORCED-REQ-RING, page 2-94	ODUK-BDI-PM, page 2-154	WVL-MISMATCH, page 2-210
FORCED-REQ-SPAN, page 2-95	ODUK-LCK-PM, page 2-155	—

2.3 Logical Object Type Definitions

ONS 15454 alarms are grouped according to their logical object types in alarm profile listings (for example OCN::LOS). Each alarm entry in this chapter lists its type. These are defined in Table 2-7.

Note Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. For example, the "OCN" logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Table 2-7 Alarm Type/Object Definition

AICI-AEP	Alarm Interface Controller–International/Alarm Expansion Panel. A combination term that refers to this platform's AIC card.
AICI-AIE	Alarm Interface Controller–International/Alarm Interface Extension. A combination term that refers to this platform's AIC-I card.
AIP	Auxiliary interface protection module.
AOTS	Amplified optical transport section.
BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CLIENT	The low-speed port, such as a transponder (TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) or muxponder (MXP_2.5G_10G), where the optical signal is dropped.
DS1	A DS-1 line on a DS-1 card.
DS3	A DS-3 line on a DS-3 card.
EC1-12	An EC1-12 line on an EC1-12 card.
ENVALRM	An environmental alarm port.
EQPT	A card in any of the eight non-common card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, STS, and VT.

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

EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
FAN	Fan-tray assembly.
FCMR	An FC_MR-4 Fibre Channel card, not currently used in this release.
FUDC	SONET F1 byte user data channel.
G1000	A G1000 Ethernet card (G1000-4).
ML100T	An ML100 card (ML100T-12).
ML1000	An ML1000 Ethernet card (ML1000-2).
NE	The entire network element.
NE-SYNCH	Represents the timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCN	An OC-N line on an OC-N card.
OMS	Optical multiplex section.
OTN	Optical transport network.
OSC-RING	Optical service channel ring.
PWR	Power.
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect).
STSTRM	STS alarm detection at termination (downstream from the cross-connect).
TRUNK	The optical or dense wavelength division multiplexing (DWDM) card carrying the high-speed signal.
UCP-IPCC	Unified control plane (UCP) communication channel.
UCP-CKT	UCP circuit.
VCG	VT concatenation.
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect).
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect).

2.4 Alarm Index by Logical Object Type

Table 2-8 gives the name and page number of every alarm in the chapter, organized by logical object type.

Note This alarm profile list is taken directly from the CTC interface. Some items do not appear in alphabetical order.

Table 2-8 Alarm Index by Alarm Type

AICI-AEP: EQPT, page 2-69	EQPT: MANRESET, page 2-146	OCN: SSM-STU, page 2-191
AICI-AEP: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT: MEA (EQPT), page 2-148	OCN: SSM-TNC, page 2-192
AICI-AIE: EQPT, page 2-69	MEM-GONE, page 2-151	OCN: SYNC-FREQ, page 2-195
AICI-AIE: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT:MEM-LOW, page 2-151	OCN: TIM, page 2-198
AIP: INVMACADR, page 2-111	EQPT: NO-CONFIG, page 2-152	OCN: WKSWPR, page 2-209
AIP: MEA (AIP), page 2-148	EQPT: PEER-NORESPONSE, page 2-166	OCN: WTR, page 2-210
AIP: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT: PROTNA, page 2-170	OMS: AS-CMD, page 2-32
AOTS: AMPLI-INIT, page 2-24	EQPT: PWR-REDUN, page 2-172	OMS: AS-MT, page 2-33
AOTS: AS-CMD, page 2-32	EQPT: RUNCFG-SAVENEED, page 2-178	OMS: OPWR-HDEG, page 2-158
AOTS: AS-MT, page 2-33	EQPT: SFTWDOWN, page 2-183	OMS: OPWR-HFAIL, page 2-160
AOTS: CASETEMP-DEG, page 2-50	EQPT: SWMTXMOD, page 2-193	OMS: OPWR-LDEG, page 2-160
AOTS: FIBERTEMP-DEG, page 2-94	EQPT: WKSWPR, page 2-209	OMS: OPWR-LFAIL, page 2-161
AOTS: GAIN-HDEG, page 2-97	EQPT: WTR, page 2-210	OMS: VOA-HDEG, page 2-207
AOTS: GAIN-HFAIL, page 2-98	EXT-SREF: FRCDSWTOPRI, page 2-95	OMS: VOA-HFAIL, page 2-208
AOTS: GAIN-LDEG, page 2-98	EXT-SREF: FRCDSWTOSEC, page 2-96	OMS: VOA-LDEG, page 2-208
AOTS: GAIN-LFAIL, page 2-99	EXT-SREF: FRCDSWTOTHIRD, page 2-96	OMS: VOA-LFAIL, page 2-209
AOTS: LASER-APR, page 2-115	EXT-SREF: MANSWTOPRI, page 2-146	OSC-RING: NTWTPINC, page 2-153
AOTS: LASERBIAS-DEG, page 2-115	EXT-SREF: MANSWTOSEC, page 2-146	OSC-RING: RING-ID-MIS, page 2-176
AOTS: LASERBIAS-FAIL, page 2-116	EXT-SREF: MANSWTOTHIRD, page 2-147	OTS: AS-CMD, page 2-32
AOTS: LASERTEMP-DEG, page 2-117	EXT-SREF: SWTOPRI, page 2-194	OTS: AS-MT, page 2-33
AOTS: OPWR-HDEG, page 2-158	EXT-SREF: SWTOSEC, page 2-194	OTS: AWG-DEG, page 2-40

Table 2-8 Alarm Index by Alarm Type (continued)

AOTS: OPWR-HFAIL, page 2-160	EXT-SREF: SWTOTHIRD, page 2-194	OTS: AWG-FAIL, page 2-40
AOTS: OPWR-LDEG, page 2-160	EXT-SREF: SYNCPRI, page 2-195	OTS: AWG-OVERTEMP, page 2-41
AOTS: OPWR-LFAIL, page 2-161	EXT-SREF: SYNCSEC, page 2-196	OTS: AWG-WARM-UP, page 2-41
AOTS: VOA-HDEG, page 2-207	EXT-SREF: SYNCTHIRD, page 2-197	OTS: LASERBIAS-DEG, page 2-115
AOTS: VOA-HFAIL, page 2-208	FAN: EQPT-MISS, page 2-70	OTS: LOS (OTS), page 2-134
AOTS: VOA-LDEG, page 2-208	FAN: FAN, page 2-83	OTS: OPWR-HDEG, page 2-158
AOTS: VOA-LFAIL, page 2-209	FAN: FANDEGRADE, page 2-84	OTS: OPWR-HFAIL, page 2-160
BITS: AIS, page 2-21	FAN: MEA (FAN), page 2-150	OTS: OPWR-LDEG, page 2-160
BITS: LOF (BITS), page 2-120	FAN: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	OTS: OPWR-LFAIL, page 2-161
BITS: LOS (BITS), page 2-127	FCMR: AS-CMD, page 2-32	OTS: SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
BITS: SSM-DUS, page 2-188	FCMR: AS-MT, page 2-33	OTS: SH-INS-LOSS-VAR-DEG-LOW, page 2-184
BITS: SSM-FAIL, page 2-189	FCMR: INC-GFP-OUTOFFRAME, page 2-107	OTS: SHUTTER-OPEN, page 2-184
BITS: SSM-OFF, page 2-189	FCMR: INC-GFP-SIGLOSS, page 2-108	OTS: VOA-HDEG, page 2-207
BITS: SSM-PRS, page 2-190	FCMR: INC-GFP-SYNCLOSS, page 2-108	OTS: VOA-HFAIL, page 2-208
BITS: SSM-RES, page 2-190	FCMR: INC-SIGLOSS, page 2-109	OTS: VOA-LDEG, page 2-208
BITS: SSM-SMC, page 2-191	FCMR: INC-SYNCLOSS, page 2-110	OTS: VOA-LFAIL, page 2-209
BITS: SSM-ST2, page 2-191	FCMR: PORT-MISMATCH, page 2-169	PWR: AS-CMD, page 2-32
BITS: SSM-ST3, page 2-192	FCMR: TPTFAIL (FC_MR-4), page 2-200	PWR: BAT-FAIL, page 2-41
BITS: SSM-ST3E, page 2-192	FUDC: AIS, page 2-21	PWR: EHIBATVG, page 2-66
BITS: SSM-ST4, page 2-192	FUDC: LOS (FUDC), page 2-131	PWR: ELWBATVG, page 2-66
BITS: SSM-STU, page 2-191	G1000: AS-CMD, page 2-32	PWR: HIBATVG, page 2-100
BITS: SSM-TNC, page 2-192	G1000: AS-MT, page 2-33	PWR: LWBATVG, page 2-145

Table 2-8 Alarm Index by Alarm Type (continued)

BITS: SYNC-FREQ, page 2-195	G1000: CARLOSS (G1000), page 2-46	STSMON: AIS-P, page 2-22
BPLANE: AS-CMD, page 2-32	G1000: LPBKFACILITY (G1000), page 2-142	STSMON: AUTOSW-AIS, page 2-36
BPLANE: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	G1000: LPBKTERMINAL (G1000), page 2-144	STSMON: AUTOSW-LOP (STSMON), page 2-37
CLIENT: AIS, page 2-21	G1000: TPTFAIL (G1000), page 2-200	STSMON: AUTOSW-PDI, page 2-38
CLIENT: ALS, page 2-23	ML1000: AS-CMD, page 2-32	STSMON: AUTOSW-SDBER, page 2-38
CLIENT: AS-CMD, page 2-32	ML1000: CARLOSS (ML100T, ML1000), page 2-49	STSMON: AUTOSW-SFBER, page 2-38
CLIENT: AS-MT, page 2-33	ML1000: TPTFAIL (ML100T, ML1000), page 2-201	STSMON: AUTOSW-UNEQ (STSMON), page 2-39
CLIENT: CARLOSS (CLIENT), page 2-43	ML100T: AS-CMD, page 2-32	STSMON: ERFI-P-CONN, page 2-71
CLIENT: EOC, page 2-66	ML100T: CARLOSS (ML100T, ML1000), page 2-49	STSMON: ERFI-P-PAYLD, page 2-71
CLIENT: EOC-L, page 2-68	ML100T: TPTFAIL (ML100T, ML1000), page 2-201	STSMON: ERFI-P-SRVR, page 2-71
CLIENT: FAILTOSW, page 2-78	MSUDC: AIS, page 2-21	STSMON: FAILTOSW-PATH, page 2-79
CLIENT: FORCED-REQ-SPAN, page 2-95	MSUDC: LOS (MSUDC), page 2-132	STSMON: FORCED-REQ, page 2-94
CLIENT: GE-OOSYNC, page 2-100	NE-SREF: FRCDSWTOINT, page 2-95	STSMON: LOCKOUT-REQ, page 2-119
CLIENT: HI-LASERBIAS, page 2-101	NE-SREF: FRCDSWTOPRI, page 2-95	STSMON: LOP-P, page 2-125
CLIENT: HI-RXPOWER, page 2-102	NE-SREF: FRCDSWTOSEC, page 2-96	STSMON: LPBKCRS, page 2-138
CLIENT: HI-TXPOWER, page 2-103	NE-SREF: FRCDSWTOTHIRD, page 2-96	STSMON: MAN-REQ, page 2-145
CLIENT: LO-RXPOWER, page 2-126	NE-SREF: FRNGSYNC, page 2-96	STSMON: PDI-P, page 2-164
CLIENT: LO-TXPOWER, page 2-137	NE-SREF: FSTSYNC, page 2-97	STSMON: PLM-P, page 2-167
CLIENT: LOCKOUT-REQ, page 2-119	NE-SREF: HLDOVRSYNC, page 2-104	STSMON: RFI-P, page 2-174
CLIENT: LOF (CLIENT), page 2-121	NE-SREF: MANSWTOINT, page 2-146	STSMON: SD-P, page 2-180

Table 2-8 Alarm Index by Alarm Type (continued)

CLIENT: LOS (CLIENT), page 2-127	NE-SREF: MANSWTOPRI, page 2-146	STSMON: SF-P, page 2-183
CLIENT: LPBKFACILITY (CLIENT, TRUNK), page 2-140	NE-SREF: MANSWTOSEC, page 2-146	STSMON: TIM-P, page 2-199
CLIENT: LPBKTERMINAL (CLIENT, TRUNK), page 2-143	NE-SREF: MANSWTOTHIRD, page 2-147	STSMON: UNEQ-P, page 2-204
CLIENT: MANUAL-REQ-SPAN, page 2-147	NE-SREF: SSM-PRS, page 2-190	STSMON: WKSWPR, page 2-209
CLIENT: OUT-OF-SYNC, page 2-164	NE-SREF: SSM-RES, page 2-190	STSMON: WTR, page 2-210
CLIENT: PORT-CODE-MISM, page 2-168	NE-SREF: SSM-SMC, page 2-191	STSTRM: AIS-P, page 2-22
CLIENT: PORT-COMM-FAIL, page 2-168	NE-SREF: SSM-ST2, page 2-191	STSTRM: AU-LOF, page 2-34
CLIENT: PORT-MISMATCH, page 2-169	NE-SREF: SSM-ST3, page 2-192	STSTRM: ERFI-P-CONN, page 2-71
CLIENT: PORT-MISSING, page 2-169	NE-SREF: SSM-ST3E, page 2-192	STSTRM: ERFI-P-PAYLD, page 2-71
CLIENT: RFI, page 2-173	NE-SREF: SSM-ST4, page 2-192	STSTRM: ERFI-P-SRVR, page 2-71
CLIENT: SD (CLIENT, TRUNK), page 2-178	NE-SREF: SSM-STU, page 2-191	STSTRM: LOM, page 2-124
CLIENT: SF (CLIENT, TRUNK), page 2-181	NE-SREF: SSM-TNC, page 2-192	STSTRM: LOP-P, page 2-125
CLIENT: SQUELCHED, page 2-187	NE-SREF: SWTOPRI, page 2-194	STSTRM: OOU-TPT, page 2-157
CLIENT: SSM-DUS, page 2-188	NE-SREF: SWTOSEC, page 2-194	STSTRM: PDI-P, page 2-164
CLIENT: SSM-FAIL, page 2-189	NE-SREF: SWTOTHIRD, page 2-194	STSTRM: PLM-P, page 2-167
CLIENT: SSM-LNC, page 2-189	NE-SREF: SYNCPRI, page 2-195	STSTRM: RFI-P, page 2-174
CLIENT: SSM-OFF, page 2-189	NE-SREF: SYNCSEC, page 2-196	STSTRM: SD-P, page 2-180
CLIENT: SSM-PRC, page 2-190	NE-SREF: SYNCTHIRD, page 2-197	STSTRM: SF-P, page 2-183
CLIENT: SSM-PRS, page 2-190	NE: APC-DISABLED, page 2-24	STSTRM: SQM, page 2-188
CLIENT: SSM-RES, page 2-190	NE: APC-FAIL, page 2-25	STSTRM: TIM-P, page 2-199
CLIENT: SSM-SDH-TN, page 2-190	NE: AS-CMD, page 2-32	STSTRM: UNEQ-P, page 2-204

Table 2-8 Alarm Index by Alarm Type (continued)

CLIENT: SSM-SETS, page 2-191	NE: AUD-LOG-LOSS, page 2-34	TRUNK: AIS, page 2-21
CLIENT: SSM-SMC, page 2-191	NE: AUD-LOG-LOW, page 2-34	TRUNK: ALS, page 2-23
CLIENT: SSM-ST2, page 2-191	NE: DATAFLT, page 2-62	TRUNK: AS-CMD, page 2-32
CLIENT: SSM-ST3, page 2-192	NE: DBOSYNC, page 2-62	TRUNK: AS-MT, page 2-33
CLIENT: SSM-ST3E, page 2-192	NE: DUP-IPADDR, page 2-65	TRUNK: CARLOSS (TRUNK), page 2-50
CLIENT: SSM-ST4, page 2-192	NE: DUP-NODENAME, page 2-65	TRUNK: DSP-COMM-FAIL, page 2-63
CLIENT: SSM-STU, page 2-191	NE: ETH-LINKLOSS, page 2-73	TRUNK: DSP-FAIL, page 2-63
CLIENT: SSM-TNC, page 2-192	NE: HITEMP, page 2-103	TRUNK: EOC, page 2-66
CLIENT: SYNC-FREQ, page 2-195	NE: I-HITEMP, page 2-105	TRUNK: EOC-L, page 2-68
CLIENT: TIM, page 2-198	NE: INTRUSION-PSWD, page 2-111	TRUNK: FAILTOSW, page 2-78
CLIENT: TIM-MON, page 2-198	NE: LAN-POL-REV, page 2-114	TRUNK: FEC-MISM, page 2-84
CLIENT: WKSWPR, page 2-209	NE: OPTNTWMIS, page 2-157	TRUNK: FORCED-REQ-SPAN, page 2-95
CLIENT: WTR, page 2-210	NE: SNTP-HOST, page 2-185	TRUNK: GCC-EOC, page 2-100
DS1: AIS, page 2-21	NE: SYSBOOT, page 2-197	TRUNK: GE-OOSYNC, page 2-100
DS1: AS-CMD, page 2-32	OCH: AS-CMD, page 2-32	TRUNK: HI-LASERBIAS, page 2-101
DS1: AS-MT, page 2-33	OCH: AS-MT, page 2-33	TRUNK: HI-RXPOWER, page 2-102
DS1: LOF (DS1), page 2-121	OCH: OPWR-HDEG, page 2-158	TRUNK: HI-TXPOWER, page 2-103
DS1: LOS (DS1), page 2-128	OCH: OPWR-HFAIL, page 2-160	TRUNK: LO-RXPOWER, page 2-126
DS1: LPBKDS1FEAC, page 2-139	OCH: OPWR-LDEG, page 2-160	TRUNK: LO-TXPOWER, page 2-137
DS1: LPBKDS1FEAC-CMD, page 2-139	OCH: OPWR-LFAIL, page 2-161	TRUNK: LOCKOUT-REQ, page 2-119
DS1: LPBKFACILITY (DS1, DS3), page 2-141	OCH: VOA-HDEG, page 2-207	TRUNK: LOF (TRUNK), page 2-124
DS1: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	OCH: VOA-HFAIL, page 2-208	TRUNK: LOM, page 2-124
DS1: RAI, page 2-172	OCH: VOA-LDEG, page 2-208	TRUNK: LOS (TRUNK), page 2-135

Table 2-8 Alarm Index by Alarm Type (continued)

DS1: RCVR-MISS, page 2-173	OCH: VOA-LFAIL, page 2-209	TRUNK: LOS-P, page 2-136
DS1: SD (DS1, DS3), page 2-178	OCHNC-CONN: OCHNC-ACTIV-FAIL, page 2-153	TRUNK: LPBKFACILITY (CLIENT, TRUNK), page 2-140
DS1: SF (DS1, DS3), page 2-182	OCHNC-CONN: OCHNC-DEACTIV-FAIL, page 2-153	TRUNK: LPBKTERMINAL (CLIENT, TRUNK), page 2-143
DS1: TRMT, page 2-201	OCHNC-CONN: OCHNC-FAIL, page 2-153	TRUNK: MANUAL-REQ-SPAN, page 2-147
DS1: TRMT-MISS, page 2-202	OCHNC-CONN: OCHNC-INC, page 2-153	TRUNK: ODUK-AIS-PM, page 2-154
DS1: TX-AIS, page 2-203	OCN: AIS-L, page 2-22	TRUNK: ODUK-BDI-PM, page 2-154
DS1: TX-RAI, page 2-203	OCN: ALS, page 2-23	TRUNK: ODUK-LCK-PM, page 2-155
DS3: AIS, page 2-21	OCN: APSB, page 2-26	TRUNK: ODUK-OCI-PM, page 2-155
DS3: AS-CMD, page 2-32	OCN: APSC-IMP, page 2-27	TRUNK: ODUK-SD-PM, page 2-156
DS3: AS-MT, page 2-33	OCN: APSCDFLTK, page 2-27	TRUNK: ODUK-SF-PM, page 2-156
DS3: DS3-MISM, page 2-64	OCN: APSCINCON, page 2-29	TRUNK: ODUK-TIM-PM, page 2-156
DS3: FE-AIS, page 2-84	OCN: APSCM, page 2-29	TRUNK: OTUK-AIS, page 2-161
DS3: FE-DS1-MULTLOS, page 2-85	OCN: APSCNMIS, page 2-30	TRUNK: OTUK-BDI, page 2-162
DS3: FE-DS1-NSA, page 2-85	OCN: APSIMP, page 2-31	TRUNK: OTUK-LOF, page 2-162
DS3: FE-DS1-SA, page 2-86	OCN: APSMM, page 2-32	TRUNK: OTUK-SD, page 2-163
DS3: FE-DS1-SNGLLOS, page 2-86	OCN: AS-CMD, page 2-32	TRUNK: OTUK-LOF, page 2-162
DS3: FE-DS3-NSA, page 2-87	OCN: AS-MT, page 2-33	TRUNK: OTUK-TIM, page 2-164
DS3: FE-DS3-SA, page 2-88	OCN: AUTOLSROFF, page 2-35	TRUNK: OUT-OF-SYNC, page 2-164
DS3: FE-EQPT-NSA, page 2-88	OCN: BLSROSYNC, page 2-43	TRUNK: PTIM, page 2-171
DS3: FE-IDLE, page 2-90	OCN: E-W-MISMATCH, page 2-73	TRUNK: RFI, page 2-173
DS3: FE-LOF, page 2-91	OCN: EOC, page 2-66	TRUNK: SD (CLIENT, TRUNK), page 2-178

Table 2-8 Alarm Index by Alarm Type (continued)

DS3: FE-LOS, page 2-91	OCN: EOC-L, page 2-68	TRUNK: SF (DS1, DS3), page 2-182
DS3: INC-ISD, page 2-109	OCN: EXERCISE-RING-FAIL, page 2-76	TRUNK: SSM-DUS, page 2-188
DS3: LOF (DS3), page 2-122	OCN: EXERCISE-SPAN-FAIL, page 2-76	TRUNK: SSM-FAIL, page 2-189
DS3: LOS (DS3), page 2-129	OCN: EXTRA-TRAF-PREEMPT, page 2-77	TRUNK: SSM-LNC, page 2-189
DS3: LPBKDS1FEAC, page 2-139	OCN: FAILTOSW, page 2-78	TRUNK: SSM-OFF, page 2-189
DS3: LPBKDS3FEAC, page 2-139	OCN: FAILTOSWR, page 2-79	TRUNK: SSM-PRC, page 2-190
DS3: LPBKDS3FEAC-CMD, page 2-140	OCN: FAILTOSWS, page 2-81	TRUNK: SSM-PRS, page 2-190
DS3: LPBKFACILITY (DS1, DS3), page 2-141	OCN: FE-FRCDWKSWPR-RING, page 2-89	TRUNK: SSM-RES, page 2-190
DS3: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	OCN: FE-FRCDWKSWPR-SPAN, page 2-89	TRUNK: SSM-SDH-TN, page 2-190
DS3: RAI, page 2-172	OCN: FE-LOCKOUTOFPR-SPAN, page 2-90	TRUNK: SSM-SETS, page 2-191
DS3: SD (DS1, DS3), page 2-178	OCN: FE-MANWKSWPR-RING, page 2-92	TRUNK: SSM-SMC, page 2-191
DS3: SF (DS1, DS3), page 2-182	OCN: FE-MANWKSWPR-SPAN, page 2-92	TRUNK: SSM-ST2, page 2-191
E1000F: AS-CMD, page 2-32	OCN: FEPRLF, page 2-93	TRUNK: SSM-ST3, page 2-192
E1000F: CARLOSS (E100T, E1000F), page 2-45	OCN: FORCED-REQ-RING, page 2-94	TRUNK: SSM-ST3E, page 2-192
E100T: AS-CMD, page 2-32	OCN: FORCED-REQ-SPAN, page 2-95	TRUNK: SSM-ST4, page 2-192
E100T: CARLOSS (E100T, E1000F), page 2-45	OCN: FULLPASSTHR-BI, page 2-97	TRUNK: SSM-STU, page 2-191
EC1-12: AIS-L, page 2-22	OCN: HI-LASERBIAS, page 2-101	TRUNK: SSM-TNC, page 2-192
EC1-12: AS-CMD, page 2-32	OCN: HI-RXPOWER, page 2-102	TRUNK: SYNC-FREQ, page 2-195
EC1-12: AS-MT, page 2-33	OCN: HI-TXPOWER, page 2-103	TRUNK: TIM, page 2-198

Table 2-8 Alarm Index by Alarm Type (continued)

EC1-12: LOF (EC1-12), page 2-123	OCN: KB-PASSTHR, page 2-114	TRUNK: TIM-MON, page 2-198
EC1-12: LOS (EC1-12), page 2-130	OCN: KBYTE-APS-CHANNEL-FAILURE, page 2-114	TRUNK: UNC-WORD, page 2-203
EC1-12: LPBKFACILITY (EC1-12), page 2-141	OCN: LASEREOL, page 2-116	TRUNK: WKSWPR, page 2-209
EC1-12: LPBKFACILITY (EC1-12), page 2-141	OCN: LKOUTPR-S, page 2-118	TRUNK: WTR, page 2-210
EC1-12: RFI-L, page 2-174	OCN: LO-RXPOWER, page 2-126	TRUNK: WVL-MISMATCH, page 2-210
EC1-12: SD-L, page 2-180	OCN: LO-TXPOWER, page 2-137	UCP-CKT: CKTDOWN, page 2-51
EC1-12: SF-L, page 2-182	OCN: LOCKOUT-REQ, page 2-119	UCP-IPCC: LMP-HELLODOWN, page 2-118
ENVALRM: EXT, page 2-77	OCN: LOF (OCN), page 2-123	UCP-IPCC: LMP-NDFAIL, page 2-118
EQPT: AS-CMD, page 2-32	OCN: LOS (OCN), page 2-132	UCP-NBR: RSVP-HELLODOWN, page 2-177
EQPT: AUTORESET, page 2-36	OCN: LPBKFACILITY (OCN), page 2-142	VCG: LOA, page 2-119
EQPT: BKUPMEMP, page 2-42	OCN: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	VCG: VCG-DEG, page 2-206
EQPT: CARLOSS (EQPT), page 2-44	OCN: MANUAL-REQ-RING, page 2-147	VCG: VCG-DOWN, page 2-207
EQPT: CLDRESTART, page 2-53	OCN: MANUAL-REQ-SPAN, page 2-147	VT-MON: AIS-V, page 2-23
EQPT: COMIOXC, page 2-54	OCN: PRC-DUPID, page 2-170	VT-MON: AUTOSW-AIS, page 2-36
EQPT: COMM-FAIL, page 2-54	OCN: RFI-L, page 2-174	VT-MON: AUTOSW-LOP (VT-MON), page 2-37
EQPT: CONTBUS-A-18, page 2-55	OCN: RING-ID-MIS, page 2-176	VT-MON: AUTOSW-UNEQ (VT-MON), page 2-39
EQPT: CONTBUS-B-18, page 2-55	OCN: RING-MISMATCH, page 2-176	VT-MON: FAILTOSW-PATH, page 2-79
EQPT: CONTBUS-IO-A, page 2-56	OCN: RING-SW-EAST, page 2-177	VT-MON: FORCED-REQ, page 2-94
EQPT: CONTBUS-IO-B, page 2-57	OCN: RING-SW-WEST, page 2-177	VT-MON: LOCKOUT-REQ, page 2-119
EQPT: CTNEQPT-MISMATCH, page 2-58	OCN: SD-L, page 2-180	VT-MON: LOP-V, page 2-125

Table 2-8 Alarm Index by Alarm Type (continued)

EQPT: CTNEQPT-PBPROT, page 2-59	OCN: SF-L, page 2-182	VT-MON: MAN-REQ, page 2-145
EQPT: CTNEQPT-PBWORK, page 2-61	OCN: SPAN-SW-EAST, page 2-185	VT-MON: UNEQ-V, page 2-206
EQPT: EQPT, page 2-69	OCN: SPAN-SW-WEST, page 2-186	VT-MON: WKSWPR, page 2-209
EQPT: ERROR-CONFIG, page 2-72	OCN: SQUELCH, page 2-186	VT-MON: WTR, page 2-210
EQPT: EXCCOL, page 2-75	OCN: SSM-DUS, page 2-188	VT-TERM: AIS-V, page 2-23
EQPT: FAILTOSW, page 2-78	OCN: SSM-FAIL, page 2-189	VT-TERM: LOM, page 2-124
EQPT: FORCED-REQ, page 2-94	OCN: SSM-OFF, page 2-189	VT-TERM: LOP-V, page 2-125
EQPT: HITEMP, page 2-103	OCN: SSM-PRS, page 2-190	VT-TERM: OOU-TPT, page 2-157
EQPT: IMPROPRMVL, page 2-105	OCN: SSM-RES, page 2-190	VT-TERM: PLM-V, page 2-167
EQPT: INHSWPR, page 2-110	OCN: SSM-SMC, page 2-191	VT-TERM: RFI-V, page 2-175
EQPT: INHSWWKG, page 2-110	OCN: SSM-ST2, page 2-191	VT-TERM: SD-P, page 2-180
EQPT: IOSCFGCOPY, page 2-113	OCN: SSM-ST3, page 2-192	VT-TERM: SF-P, page 2-183
EQPT: LOCKOUT-REQ, page 2-119	OCN: SSM-ST3E, page 2-192	VT-TERM: SQM, page 2-188
EQPT: MAN-REQ, page 2-145	OCN: SSM-ST4, page 2-192	VT-TERM: UNEQ-V, page 2-206

2.5 Trouble Notifications

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 reports alarmed trouble notifications and Not-Alarmed (NA) notifications, if selected, in the CTC Alarms window. Alarms typically signify a problem that the user needs to fix, such as a loss of signal (LOS), while Not-Alarmed (NA) notifications do not necessarily need immediate troubleshooting.

Telcordia further divides alarms into Service-Affecting (SA) and NSA status. A Service-Affecting (SA) failure affects a provided service or the network's ability to provide service. For example, the "TRMT-MISS" alarm on page 2-202 is characterized by default as an SA failure. TRMT-MISS occurs when a cable connector is removed from an active DS-1 card port. The default severity assumes that service has been interrupted or moved. If the DS-1 card is in a protection group and the traffic is on the protect card rather than the working card, or if the port with the TRMT-MISS alarm has no circuits provisioned, TRMT-MISS would be raised as NSA because traffic was not interrupted or moved.

2.5.1 Conditions

The term "Condition" refers to any problem detected on an ONS 15454 shelf whether or not the problem is reported (that is, whether or not it generates a trouble notification). Reported conditions include alarms, Not-Alarmed conditions, and Not-Reported (NR) conditions. A snapshot of all current raised conditions on a node, whether they are reported or not, can be retrieved using the CTC Conditions window or using TL1's set of RTRV-COND commands. You can see the actual reporting messages for alarms and NAs in the CTC History tab.

For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

2.5.2 Severities

The ONS 15454 uses Telcordia standard severities: Critical (CR), Major (MJ), and Minor (MN). Non-Service Affecting (NSA) alarms always have a Minor (MN) severity. Service-Affecting (SA) alarms can be Critical (CR), Major (MJ), or Minor (MN). Critical alarms generally indicate severe, service-affecting trouble that needs immediate correction. A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For SONET signal alarms, loss of traffic on more than five DS-1 circuits is Critical. Loss of traffic on one to five DS-1 circuits is Major (MJ). Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.

An example of a Non-Service Affecting (NSA) alarm is the "FSTSYNC" condition on page 2-97 (Fast Start Synchronization Mode), which indicates the ONS 15454 is choosing a new timing reference because the previously used reference has failed. The user needs to troubleshoot the loss of the prior timing source, but the loss is not immediately disruptive to service.

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

This chapter lists the default profile alarm severity for the Service-Affecting (SA) case of each alarm when it is applicable. Any alarm with a profile value of Critical (CR) or Major (MJ) will, if reported as Non-Service Affecting (NSA) because no traffic is lost, be reported with a Minor (MN) severity instead, in accordance with Telcordia rules.

2.6 Safety Summary

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

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

Some troubleshooting procedures require installation or removal of OC-192 cards; in these instances users should pay close attention to the following warnings.

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

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

Warning **Class 1 laser product.**

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

2.7 Alarm Procedures

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

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner is not indented. If it is, click it to turn it off. When you are done checking for alarms, click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the *Cisco ONS 15454 Procedure Guide*.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the *Cisco ONS 15454 Procedure Guide*.

2.7.1 AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, DS1, DS3, FUDC, MSUDC, TRUNK

Note The MSUDC object is not supported in this platform in this release. It is reserved for future development.

The Alarm Indication Signal (AIS) condition indicates that this node is detecting AIS in the incoming signal SONET overhead.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Note DS-3 and EC-1 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-132, or out-of-service (OOS) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.2 AIS-L

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

The AIS Line (AIS-L) condition indicates that this node is detecting line-level AIS in the incoming signal.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.3 AIS-P

- Not Reported (NR), Non-Service Affecting (NSA)

- Logical Objects: STSMON, STSTRM

The AIS Path (AIS-P) condition means that this node is detecting AIS in the incoming path.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.4 AIS-V

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: VT-MON, VT-TERM

The AIS Virtual Tributary (VT) condition (AIS-V) means that this node is detecting AIS in the incoming VT-level path.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

See the "AIS-V on DS3XM-6 Unused VT Circuits" section on page 1-89 for more information.

Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.5 ALS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition occurs when a DWDM amplifier (OPT-BST or OPT-PRE) is switched on. The turn-on process lasts approximately nine seconds, and the condition clears after approximately 10 seconds.

Note ALS is an informational condition. It does not require troubleshooting.

2.7.6 AMPLI-INIT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Amplifier Initialized (AMPLI-INIT) condition occurs when a DWDM amplifier card (OPT-BST or OPT-PRE) is not able to calculate gain. This condition is typically raised with the "APC-DISABLED" alarm on page 2-24.

Clear the AMPLI-INIT Condition

Step 1 Complete the "Delete a Circuit" procedure on page 2-217 on the most recently created circuit.

Step 2 Recreate this circuit using the procedures in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.7 APC-DISABLED

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Automatic Power Control (APC) Disabled (APC-DISABLED) alarm occurs when the information related to the number of channels is not reliable. The alarm can occur when the any of the following alarms also occur: the "EQPT" alarm on page 2-69, the "IMPROPRMVL" alarm on page 2-105, or the "MEA (EQPT)" alarm on page 2-148. If the alarm occurs with the creation of the first circuit, delete and recreate it.

Clear the APC-DISABLED Alarm

Step 1 Complete the appropriate procedure to clear the main alarm:

- Clear the EQPT Alarm, page 2-70
- Clear the IMPROPRMVL Alarm, page 2-106
- Clear the MEA (EQPT) Alarm, page 2-148

Step 2 If the alarm does not clear, complete the "Delete a Circuit" procedure on page 2-217 and then recreate it.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.8 APC-FAIL

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Failure (APC-FAIL) alarm occurs when APC has not been able to create a setpoint on a node because it has exceeded all allocated power margins including gain, power, or attenuation. These power margins (from 0 dB to 3 dB) are allocated when the network is installed. Margins can be consumed due to fiber aging or the insertion of unexpected extra loss in the span after a fiber cut.

Clear the APC-FAIL Alarm

Step 1 Determine whether the increased margin use is due to fiber aging:

a. Complete the task for checking OSC span attenuation in the *Cisco ONS 15454 Procedure Guide* Chapter 7, "Turn Up DWDM Network."

b. Obtain the original MetroPlanner *.cmn file, then cross-reference original span values with current ones (obtained in CTC) to determine whether a loss of 0 dB to 3dB or more has occurred across the questioned span. To obtain current values, complete the procedure for verifying optical receive power in the *Cisco ONS 15454 Procedure Guide* Chapter 7, "Turn Up DWDM Network."

c. On the degraded span, test fiber integrity by using optical testing equipment to verify port levels. Then verify these levels against each termination listed in CTC. To do this, complete the task for verifying DWDM card parameters in the *Cisco ONS 15454 Procedure Guide* Chapter 7, "Turn Up DWDM Network."

Note Throughout this trouble isolation process, ensure that safe and proper fiber cleaning and scoping procedures are used. Follow established site practices or, if none exists, complete the procedure for cleaning fiber connectors in the *Cisco ONS 15454 Procedure Guide* Chapter 17, "Maintain the Node."

Step 2 If the span problem is due to aged fiber, replace it by completing the task to install fiber optic cables on DWDM cards in the *Cisco ONS 15454 Procedure Guide* Chapter 2, "Install Cards and Fiber-Optic Cable."

Step 3 If the trouble is not due to aging but to a fiber cut:

a. Verify the alarms by completing the procedure for viewing alarms, history, events and conditions in the Cisco ONS 15454 Procedure Guide Chapter 9, "Manage Alarms."

b. Complete the procedures in the "Identify Points of Failure on an Optical Circuit Path" section on page 1-37.

c. Resolve the issue and alarm by completing the procedure to verify the optical receive power in the *Cisco ONS 15454 Procedure Guide* Chapter 7, "Turn Up DWDM Network."

d. If the LOS alarm is raised against a relevant OCN object, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.9 APSB

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Automatic Protection Switching (APS) Channel Byte Failure (APSB) alarm occurs when line terminating equipment detects protection switching byte failure or an invalid code in the incoming APS signal. Some older, non-Cisco SONET nodes send invalid APS codes if they are configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15454. These invalid codes causes an APSB on an ONS node.

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. Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.10 APSC-IMP

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An Improper APS Code (APSC-IMP) alarm indicates bad or invalid K bytes. APSC-IMP occurs on OC-N cards in an MS-SPRing configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. 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 at the lower-right outside edge of the shelf assembly.

Note This alarm can occur when the exercise command or a Lock Out is applied to a span. An externally switched span does not raise this alarm because traffic is preempted.

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 is with 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, complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213.

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

Step 4 If a node has a ring name number that does not match the other nodes, complete the "Change a BLSR Ring Name" procedure on page 2-213 to make the ring names identical.

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

2.7.11 APSCDFLTK

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Default K Byte Received (APSCDFLTK) alarm occurs when a bidirectional line switched ring (BLSR) is not properly configured, for example, when a four-node BLSR has one node configured as a path protection. When this misconfiguration occurs, a node in a path protection or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for the "BLSROSYNC" alarm on page 2-43.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213 to verify that each node has a unique node ID number.

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

Step 3 If two nodes have the same node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-214 to change one node's ID number so that each node ID is unique.

Step 4 If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the "E-W-MISMATCH" alarm on page 2-73.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 Procedure Guide* provides a procedure for fibering BLSRs.

Step 5 If the alarm does not clear and if the network is a four-fiber BLSR, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protection fiber.

Step 6 If the alarm does not clear, complete the "Verify Node Visibility for Other Nodes" procedure on page 2-214.

Step 7 If nodes are not visible, complete the "Verify or Create Node DCC Terminations" procedure on page 2-214 to ensure that SONET data communications channel (DCC) terminations exist on each node.

Step 8 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.12 APSC-IMP

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An Improper SONET APS Code (APSC-IMP) alarm indicates bad or 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. 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 at the lower-right outside edge of the shelf assembly.

Note This alarm can occur on a virtual tributary (VT) tunnel when it does not have VT circuits provisioned. It can also occur when the exercise command or a lockout is applied to a span. An externally switched span does not raise this alarm because traffic is preempted.

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 is with 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 name that matches the other node ring names. Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213.

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

Step 4 If a node has a ring name that does not match the other nodes, make the ring name of that node identical to the other nodes. Complete the "Change a BLSR Ring Name" procedure on page 2-213.

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

2.7.13 APSCINCON

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

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

Clear the APSCINCON Alarm

Step 1 Look for other alarms, especially the "LOS (OCN)" alarm on page 2-132, the "LOF (OCN)" alarm on page 2-123, or the "AIS" alarm on page 2-21. Clearing these alarms clears the APSCINCON alarm.

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

2.7.14 APSCM

- Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The APS Channel Mismatch (APSCM) 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 does not occur. The APSCM alarm occurs only on the ONS 15454 when bidirectional protection is used on OC-N cards in a 1+1 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.15 APSCNMIS

- Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The APS Node ID Mismatch (APSCNMIS) alarm occurs when the source node ID contained in the SONET K2 byte of the incoming APS channel is not present in the ring map. The APSCNMIS alarm could occur and clear when a BLSR is being provisioned. If so, you can disregard the temporary occurrence. If the APSCNMIS remains, the alarm clears when a K byte with a valid source node ID is received.

Clear the APSCNMIS Alarm

Step 1 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213 to verify that each node has a unique node ID number.

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

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

Step 4 If two nodes have the same node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-214 to change one node's ID number so that each node ID is unique.

Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. The BLSR window shows the node ID of the login node.

Note Applying and removing a lockout on a span causes the ONS 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 2-215 to lock out the span.

Step 6 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215 to clear the lockout.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.16 APSIMP

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Invalid Code (APSIMP) condition occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for path protection or BLSR protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the proper type of byte.

The condition is superseded by an APS, APSCM, or APSMM. It is not superseded by AIS or RDI line alarms. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Condition

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Step 3 Ensure that both protect ports are configured for SONET.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.17 APSMM

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An APS Mode Mismatch (APSMM) 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.

Clear the APSMM Alarm

Step 1 For the reporting ONS 15454, display node view and verify the protection scheme provisioning.

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

b. Click the 1+1 protection group configured for the OC-N cards.

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

Click **Edit**.

Record whether the Bidirectional Switching check box is checked.

Step 2 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 3 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1. If not, change it to match.

Step 4 Click **Apply**.

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

2.7.18 AS-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, BPLANE, CLIENT, DS1, DS3, E100T, E1000F, EC1-12, EQPT, FCMR, G1000, ML100T, ML1000, NE, OCH, OCN, OMS, OTS, PWR, TRUNK

The Alarms Suppressed by User Command (AS-CMD) condition applies to the network element (NE object), backplane, a single card, or a port on a card. It occurs when alarms are suppressed for that object and its subordinate objects; that is, suppressing alarms on a card also suppresses alarms on its ports.

Clear the AS-CMD Condition

Step 1 For all nodes, in node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column, and note what entity the condition is reported against, such as a port, slot, or shelf.

If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.

If the condition is reported against the backplane, go to Step 7.

If the condition is reported against the NE object, go to Step 8.

Step 3 Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:

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

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

- If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
- If the Suppress Alarms column check box is not checked for a port row, click **View > Go to Previous View**.

Step 4 If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 5 Locate the row number for the reported card slot.

Step 6 Click the Suppress Alarms column check box to deselect the option for the card row.

Step 7 If the condition is reported for the backplane, the alarms are suppressed for cards such as the AIP that are not in the optical or electrical slots. To clear the alarm:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. In the backplane row, deselect the Suppress Alarms column check box.

c. Click **Apply**.

Step 8 If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

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

c. Click **Apply**.

Step 9 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.19 AS-MT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, CLIENT, DS1, DS3, EC1-12, FCMR, G1000, OCH, OCN, OMS, OTS, TRUNK

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

Clear the AS-MT Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.20 AUD-LOG-LOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Loss (AUD-LOG-LOSS) condition occurs when the log is 100 percent full and that the oldest entries are being replaced as new entries are generated. The log capacity is 640 entries. You will have to off-load (save) the log to make room for more entries.

Clear the AUD-LOG-LOSS Condition

Step 1 In node view, click the **Maintenance > Audit** tabs.

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not have to assign an extension to the file. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**.

The 640 entries will be saved in this file. New entries will continue with the next number in the sequence, rather than starting over.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.21 AUD-LOG-LOW

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Low (AUD-LOG-LOW) condition occurs when the audit trail log is 80 percent full.

Note AUD-LOG-LOW is an informational condition. It does not require troubleshooting.

2.7.22 AU-LOF

The AU-LOF condition is not used in this platform in this release. It is reserved for future development.

2.7.23 AUTOLSROFF

- Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The Auto Laser Shutdown (AUTOLSROFF) alarm occurs when the OC-192 card temperature exceeds 194 degrees F (90 degrees C). The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.

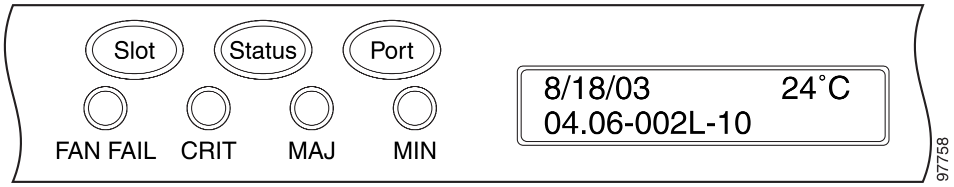
Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

Clear the AUTOLSROFF Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-1).

Figure 2-1 Shelf LCD Panel



Step 2 If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-103.

Step 3 If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Card" procedure on page 2-219 for the OC-192 card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 4 If card replacement does not clear the alarm, call Cisco TAC (1 800 553-2447) to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

2.7.24 AUTORESET

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Automatic System Reset (AUTORESET) 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.

Clear the AUTORESET Alarm

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.25 AUTOSW-AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The Automatic path protection Switch Caused by AIS (AUTOSW-AIS) condition indicates that automatic path protection protection switching occurred because of an AIS condition. The path protection is configured for revertive switching and reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.26 AUTOSW-LOP (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic UPSR Switch Caused by Loss of Pointer (LOP) condition (AUTOSW-LOP) for the STS monitor (STSMON) indicates that automatic path protection protection switching occurred because of the "LOP-P" alarm on page 2-125. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-125.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.27 AUTOSW-LOP (VT-MON)

- Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

The AUTOSW-LOP alarm for the virtual tributary monitor (VT-MON) indicates that automatic path protection protection switching occurred because of the "LOP-V" alarm on page 2-125. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (VT-MON) Alarm

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-126.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.28 AUTOSW-PDI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic UPSR Switch Caused by Payload Defect Indication (PDI) condition (AUTOSW-PDI) indicates that automatic path protection switching occurred because of a "PDI-P" alarm on page 2-164. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-165.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.29 AUTOSW-SDBER

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic UPSR Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition (AUTOSW-SDBER) indicates that a signal degrade [see the "SD (CLIENT, TRUNK)" condition on page 2-178] caused automatic path protection protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.30 AUTOSW-SFBER

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition (AUTOSW-SFBER) indicates that the "SF (DS1, DS3)" condition on page 2-182 caused automatic path protection protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF (DS1, DS3) Condition" procedure on page 2-182.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.31 AUTOSW-UNEQ (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

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

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-204.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.32 AUTOSW-UNEQ (VT-MON)

- Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

AUTOSW-UNEQ (VT-MON) indicates that the "UNEQ-V" alarm on page 2-206 alarm caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (VT-MON) Alarm

Step 1 Complete the "Clear the UNEQ-V Alarm" procedure on page 2-206.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.33 AWG-DEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The arrayed waveguide gratings (AWG) Temperature Degrade alarm (AWG-DEG) indicates that an internal failure on the multiplexer or demultiplexer heater control circuit causes the AWG temperature to rise above or fall below the degrade threshold.

Clear the AWG-DEG Alarm

Step 1 This alarm does not immediately affect traffic. But eventually, you will need to complete the "Physically Replace a Card" procedure on page 2-219 on the reporting card to clear the alarm.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.34 AWG-FAIL

- Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The AWG Temperature Fail (AWG-FAIL) alarm indicates that a heater control circuit on the multiplexer or demultiplexer card has failed.

Clear the AWG-FAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.35 AWG-OVERTEMP

- Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The AWG Over Temperature (AWG-OVERTEMP) alarm occurs in conjunction with the "AWG-FAIL" alarm on page 2-40 when the AWG temperature exceeds 100 degrees C (212 degrees F). The multiplexer or demultiplexer goes into protection mode, disabling the AWG chip heater.

Clear the AWG-OVERTEMP Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.36 AWG-WARM-UP

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The AWG Warm-up (AWG-WARM-UP) condition occurs during AWG startup. The length of time needed for the condition to clear varies, depending upon environmental conditions. It can last up to approximately 10 minutes.

Note AWG-WARM-UP is an informational condition, and does not require troubleshooting unless it does not clear.

2.7.37 BAT-FAIL

- Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The Battery Fail (BAT-FAIL) alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so on-site information about the conditions is necessary for troubleshooting.

Clear the BAT-FAIL Alarm

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.38 BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Primary Non-Volatile Backup Memory Failure (BKUPMEMP) alarm refers to a problem with the TCC2 card's flash memory. The alarm occurs when the TCC2 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 verify for errors in data transmitted to the TCC2.

The BKUPMEMP alarm can also cause the "EQPT" alarm on page 2-69. 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 TCC2 card.

Clear the BKUPMEMP Alarm

Step 1 Verify that both TCC2 cards are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2 cards.

Step 2 If both TCC2 cards are powered and enabled, reset the TCC2 card against which the alarm is raised. If the card is the active TCC2 card, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217. If the card is the standby TCC2, use the substeps below.

a. Right-click the standby TCC2 card in CTC.

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

c. Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.

d. Wait ten minutes to verify that the card you reset completely reboots.

Step 3 If the TCC2 you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.39 BLSROSYNC

- Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The BLSR Out Of Synchronization (BLSROSYNC) alarm occurs when you attempt to add or delete a circuit and a node on a working ring loses its DCC connection because all transmit and receive fiber has been removed. CTC cannot generate the ring table and causes the BLSROSYNC alarm.

Clear the BLSROSYNC Alarm

Step 1 Reestablish cabling continuity to the node reporting the alarm. Refer to the *Cisco ONS 15454 Procedure Guide* for cabling information.

When the DCC is established between the node and the rest of the BLSR, it becomes visible to the BLSR and should be able to function on the circuits.

Step 2 If alarms occur when you have provisioned the DCCs, see the "EOC" section on page 2-66.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.40 CARLOSS (CLIENT)

- Major (MJ), Service-Affecting (SA)
- Logical Object: CLIENT

A Carrier Loss (CARLOSS) alarm on the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card occurs when ITU-T G.709 monitoring is turned off at the client port. It is similar to the "LOS (OCN)" alarm on page 2-132.

Clear the CARLOSS (CLIENT) Alarm

Step 1 From node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card to display card view.

Step 2 Click the **Provisioning > OTN > OTN Lines** tabs.

Step 3 Check the check box under the **G.709 OTN** column.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.41 CARLOSS (EQPT)

- Major (MJ), Service-Affecting (SA)
- Logical Object: EQPT

A CARLOSS on Equipment alarm generally occurs on OC-N cards when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC2 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.

Clear the CARLOSS (EQPT) Alarm

Step 1 If the reporting card is a TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card, verify the type of payload configured:

a. Double-click the reporting TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card.

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

c. From the Payload Data Type list, choose the correct payload for the card and click **Apply**.

Step 2 If the reporting card is an OC-N card, verify connectivity by pinging the ONS 15454 that is reporting the alarm:

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

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

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

```
ping ONS-15454-IP-address
```

For example:

```
ping 198.168.10.10.
```

If the workstation has connectivity to the ONS 15454, it shows a "reply from *IP-Address*" after the ping. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 3 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 4 Using optical test equipment, verify that proper receive levels are achieved.

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port.

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC.

Step 9 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.42 CARLOSS (E100T, E1000F)

- Major (MJ), Service-Affecting (SA)
- Logical Objects: E100T, E1000F

A CARLOSS on the LAN E100T or E1000F Ethernet (traffic) card is the data equivalent of the "LOS (OCN)" alarm on page 2-132. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface Converter (GBIC) fiber connected to an optical (traffic) card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled (in service, IS) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP). 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.

Clear the CARLOSS (E100T, E1000F) Alarm

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

Step 2 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to an OC-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.

Step 4 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port.

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

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

Step 6 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the Ethernet (traffic) card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 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.

If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps unless the Ethernet circuit is part of a manual cross-connect:

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

b. Click **Select Affected Circuits** in the shortcut menu that appears.

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

d. From the examination of the layout of your network, determine which ONS 15454 and card 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 connects the Ethernet card to an OC-N card at the same node.

e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-217 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 9 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.43 CARLOSS (G1000)

- Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

A CARLOSS on the LAN G1000 Ethernet (traffic) card is the data equivalent of the "LOS (OCN)" condition on page 2-132. The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-4 card is caused by one of two situations:

- The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting G1000-4 card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause

is cleared, the far-end G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as the "TPTFAIL (G1000)" alarm on page 2-200 or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G-Series) alarm.

Refer to the *Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" alarm on page 2-201 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 (in service, IS) 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.

Clear the CARLOSS (G1000) Alarm

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

Step 2 If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 Verify that optical receive levels are within the normal range.

Step 5 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 6 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port.

Step 7 If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the G1000-4 card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail:

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

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

Step 8 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 9 If the alarm does not clear and the "TPTFAIL (G1000)" alarm on page 2-200 is also reported, complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-200. 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 could be the G1000-4's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 10 If the TPTFAIL alarm was not reported, determine whether a terminal (inward) loopback has been provisioned on the port:

a. In node view, click the card to go to card view.

b. Click the **Conditions** tab and the **Retrieve Conditions** button.

c. If LPBKTERMINAL is listed for the port, a loopback is provisioned. Go to Step 11. If IS is listed, go to Step 12.

Step 11 If a loopback was provisioned, complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

On the G1000-4 card, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 port detects the termination.

If the does not have a LPBKTERMINAL condition, continue to Step 12.

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect.

Note An Ethernet manual cross-connect is used when another vendors' equipment sits between ONS 15454s, and the Open System Interconnection/Target Identifier Address Resolution Protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

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

b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.

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

d. Examine the layout of your network and determine which ONS 15454 and card 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 (traffic) card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-217 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 13 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219.

Step 14 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 15 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.44 CARLOSS (ML100T, ML1000)

- Major (MJ), Service-Affecting (SA)
- Logical Objects: ML100T, ML1000

A CARLOSS on the ML100T or ML1000 Ethernet (traffic) card is the data equivalent of the "LOS (OCN)" alarm on page 2-132. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the IOS command line interface (CLI) as a no-shutdown port and one of the following items also occurs:

- The cable is not properly connected to the near or far port.
- Auto-negotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

For information about provisioning ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6.*

Clear the CARLOSS (ML100T, ML1000) Alarm

Step 1 Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port.

Step 2 If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.

Step 3 If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.

Step 4 If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

Step 5 If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the IOS CLI. Autonegotiation will restart.

Step 6 If the alarm does not clear, complete the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8.

Step 7 If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219.

Step 8 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.45 CARLOSS (TRUNK)

- Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

A CARLOSS on the optical trunk connecting to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards is raised when ITU-T G.709 monitoring is disabled.

Clear the CARLOSS (TRUNK) Alarm

Step 1 Complete the "Clear the CARLOSS (CLIENT) Alarm" procedure on page 2-43.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.46 CASETEMP-DEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Case Temperature Degrade (CASETEMP-DEG) alarm occurs when a card detects a case temperature value outside the desired range (–5 to 65 degrees C or 23 to 149 degrees F).

Clear the CASETEMP-DEG Alarm

Step 1 If a FAN alarm is also reported, complete the "Clear the FAN Alarm" procedure on page 2-83.

Step 2 If no FAN alarm is reported, complete the "Replace the Air Filter" procedure on page 3-5.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.47 CKTDOWN

- Critical (CR), Service-Affecting (SA)
- Logical Object: UCP-CKT

The unified control plane (UCP) Circuit Down (CKTDOWN) alarm applies to logical circuits created within the UCP between devices. It occurs when there is signaling failure across a UCP interface. The failure can be caused by a number of things, such as failure to route the call within the core network. In that case, the alarm cannot be resolved from the ONS 15454 because it is an edge device.

Clear the CKTDOWN Alarm

Step 1 Ensure that the channel to neighbor has been provisioned with the correct IP address:

a. In node view, click the **Provisioning > UCP > Neighbor** tabs.

b. View the entries to find out whether the node you are trying to contact is listed.

The node name is listed under the Name column and the IP address is listed under the Node ID column. If the Node ID says 0.0.0.0 and the Enable Discovery check box is selected, the node could not automatically identify the IP address. Ping the node to ensure that it is physically and logically accessible.

c. Click **Start > Programs > Accessories > Command Prompt** to open an MS-DOS command window for pinging the neighbor.

d. At the command prompt (C:\>), type:

```
ping {node-DNS-name | node-IP-address}
```

If you typed the domain name services (DNS) name and the ping was successful, you will see:

```
pinging node-dns-name.domain-name.com. node-IP-address with 32 bytes of data:
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60

Ping statistics for IP-address:
Packets sent = 4 Received = 4 Lost = 0 (0% lost),
Approximate round trip time in milli-seconds:
Minimum = minimum-ms, Maximum = maximum-ms, Average = average-ms
```

If you typed the IP address and the ping command is successful, the result will look similar but will not include the DNS name in the first line.

e. If your DNS name or IP address ping was successful, IP access to the node is confirmed, but your neighbor configuration is wrong. Delete the neighbor by selecting it in the window and clicking **Delete**.

f. If the ping was unsuccessful, you will receive the following reply for each try:

```
Request timed out.
```

A negative reply indicates that the neighbor node is not physically or logically accessible. Resolve the access problem, which is probably a cabling issue.

Step 2 If the neighbor has not been provisioned, or if you had to delete the neighbor, create one:

a. In the Provisioning > UCP > Neighbor tabs, click the **Create** button.

b. In the Neighbor Discovery window, enter the node's DNS node name in the Neighbor Name field. Leave the Enable Discovery check box checked (default setting) if you want the neighbor to be discovered through the network.

c. Click **OK**.

The node is listed in the Neighbor column list. If the neighbor discovery worked, the neighbor IP address is listed in the Node ID column. If it is not successful, the column lists 0.0.0.0.

Step 3 If neighbor discovery is enabled, ensure that the neighbor node ID and remote Internet protocol (IP) control channel (IPCC) have been discovered correctly.

Step 4 Click the **Provisioning > UCP > IPCC** tabs and view the IPCC listing. If the IPCC has been created correctly, the Remote IP column contains the neighbor's IP address.

Step 5 If the neighbor IP address is not correctly discovered, the field contains 0.0.0.0.

a. Click the entry to select the neighbor IP address and click **Delete**.

b. If you get an error that will not allow you to delete the IPCC, you must delete the neighbor and recreate it. Click the **Neighbor** tab.

c. Click to select the neighbor and click **Delete**.

d. Go back to Step 2 to recreate the neighbor.

Step 6 If remote IPCC has not been discovered, or if it had to be deleted, create the connection:

a. In the Provisioning > UCP > IPCC tabs, click **Create**.

b. In the Unified Control Plane Provisioning window, click **Next**.

c. If no IPCCs are listed, click **Create**.

d. In the Create New IPCC window, click the DCC termination corresponding to the core network interface.

Leave the SDCC radio button selected (as long as DCCs have been created on the node) and leave the Leave Unchanged radio button selected.

e. Click **OK**. The IPCC is listed in the Unified Control Plane Provisioning window.

f. Click the neighbor to select it, and click **Next**.

g. Choose the UCP interface [for example, Slot 5 (OC-48), port 1] where the core network is connected from the pull-down menu. The field default is the node where you are logged in.

h. Choose the UCP interface TNA address type. The default is IPv4. The address field lists the login node IP address by default.

i. Click **Finish**. If creation is successful, the Remote ID column in the IPCC tab will contain the neighbor's IP address.

Step 7 Ensure that the local and remote interface IDs have been provisioned correctly:

a. Click the **Interface** tab. View the slot and port listed in the Interface column [for example, Slot 5 (OC48), port 1].

b. Compare the listed interface listed with the IPCC tab SDCC column entry.

Step 8 If the Interface column is not the same as the SDCC column entry, click the entry in the Interface window to select it and click **Delete**.

Step 9 Click **Next**.

Step 10 In the Existing CCIDs list, click the IPCC containing the DCC connection. Click **Next**.

The correct interface for the selected CCID is shown in the UPC Interface field, and the correct IP address information for the login node is shown by default in the other fields. Click **Finish**.

Step 11 If you completed all of these steps and verified the information, the alarm could be the result of a misconfiguration in the core network. Contact the core site administrators.

Step 12 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.48 CLDRESTART

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Cold Restart (CLDRESTART) condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 is first powered 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 at the lower-right outside edge of the shelf assembly.

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 2-219.

Step 2 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.49 COMIOXC

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure (COMIOXC) alarm is caused by the XC10G cross-connect card. It occurs when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 on the reporting XC10G cross-connect card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 3 If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the "Side Switch the Active and Standby XC10G Cross-Connect cards" procedure on page 2-216.

Step 4 Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting cross-connect card.

Step 5 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.50 COMM-FAIL

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Plug-In Module (card) Communication Failure (COMM-FAIL) alarm indicates that there is a communication failure between the TCC2 and the card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.51 CONTBUS-A-18

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from TCC2 A Slot to TCC2 Slot A (CONTBUS-A-18) alarm occurs when the main processor on the TCC2 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 Active TCC2 Card and Activate Standby Card" procedure on page 2-217 to make the TCC2 in Slot 11 active.

Step 2 Wait approximately 10 minutes for the TCC2 in Slot 7 to reset as the standby TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

Step 3 Position the cursor over the TCC2 card in Slot 11 and complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 to make the standby TCC2 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 TCC2" procedure on page 2-218. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.52 CONTBUS-B-18

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from TCC2 B Slot to TCC2 B Slot (CONTBUS-B-18) alarm occurs when the main processor on the TCC2 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 TCC2 card in Slot 11 and complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 to make the TCC2 in Slot 7 active.

Step 2 Wait approximately 10 minutes for the TCC2 in Slot 11 to reset as the standby TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

Step 3 Position the cursor over the TCC2 card in Slot 7 and complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 to make the standby TCC2 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 "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.53 CONTBUS-IO-A

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCC A to Shelf Slot Communication Failure (CONTBUS-IO-A) alarm occurs when the active TCC2 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 TCC2 card. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2 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 (EQPT)" alarm on page 2-148 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby TCC2 in Slot 11, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-218. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 3 If the alarm object is the standby TCC2 in Slot 11, perform a soft reset of this card:

a. Right-click the Slot 11 TCC2 card.

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

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

Step 4 If CONTBUS-IO-A is raised on several cards at once, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 7 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 TCC2" procedure on page 2-218. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.54 CONTBUS-IO-B

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCC B to Shelf Slot Communication Failure (CONTBUS-IO-B) alarm occurs when the active TCC2 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 TCC2 card. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2 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 (EQPT)" alarm on page 2-148 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby TCC2 in Slot 7, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-218. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 3 If the alarm object is the standby TCC2 in Slot 7, perform a soft reset of this card:

a. Right-click the Slot 7 TCC2 card.

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

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

Step 4 If CONTBUS-IO-B is raised on several cards at once, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 7 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 TCC2" procedure on page 2-218. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.55 CTNEQPT-MISMATCH

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Connection Equipment Mismatch (CTNEQPT-MISMATCH) condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually present in the shelf. For example, an XC card may be preprovisioned in Slot 10, but an XCVT may be physically installed.

The alarm is raised against a card that is mismatched with the card. For example, CTNEQPT-MISMATCH is raised in the following situations:

- An XC card is replaced with an XCVT or XC10G card.
- An XCVT card is replaced with an XC10G card.

Note Cisco does not support configurations of unmatched cross-connect cards in Slot 8 and Slot 10, although this situation may briefly occur during the upgrade process. (For example, you might have an XC in Slot 8 and an XC10G in Slot 10 while you are upgrading Slot 10.)

Note The cross-connect card you are replacing should not be the active card. (It can be in SBY state or otherwise not in use.)

If you upgrade a node to R4.6 and replace an XC with XCVT or XC10G, or an XCVT with an XC10G, the CTNEQPT-MISMATCH condition is raised but it will be cleared when the upgrade process ends.

Note During an upgrade, this condition occurs and is raised as its default severity, Not Alarmed (NA). However, after the upgrade has occurred, if you wish to change the condition's severity so that it is Not Reported (NR), you can do this by modifying the alarm profile used at the node. For more information about modifying alarm severities, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the CTNEQPT-MISMATCH Condition

Step 1 Verify what card is preprovisioned in the slot:

a. In node view, click the **Inventory** tab.

b. View the slot's row contents in the **Eqpt Type** and **Actual Eqpt Type** columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot. For example, Slot 8 might be provisioned for an XCVT card, which is shown in the Eqpt Type column, but an XC10G card could be physically present in the slot. The XC10G would be shown in the Actual Eqpt Type column.)

Step 2 Complete the "Physically Replace a Card" procedure on page 2-219 for the mismatched card.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.56 CTNEQPT-PBPROT

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus (CTNEQPT-PBPROT) alarm indicates a failure of the main payload between the Slot 10 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card, the reporting traffic card, the TCC2 card, or the backplane.

Note If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218 for the standby TCC2 card. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-219 for the standby TCC2 card. Do not physically reseat an active TCC2 card. Reseating the TCC2 disrupts traffic.

Note This alarm automatically raises and clears when the Slot 8 XC10G cross-connect card is reseated.

Caution It can take up to 30 minutes for software to be updated on a standby TCC2 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 CTNEQPT-PBPROT Alarm

Step 1 Perform a CTC reset on the standby XC10G cross-connect card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-218. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

If the cross-connect reset is not complete and error-free or if the TCC2 reboots automatically, call Cisco TAC (1 800 553-2447).

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the standby cross-connect card.

Step 4 Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.

Step 5 If the reporting traffic card is the active card in the protection group, complete the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 6 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 on the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 7 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 8 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 9 Complete the "Clear a Protection Group External Switching Command" procedure on page 2-216.

Step 10 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 11 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.57 CTNEQPT-PBWORK

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus (CTNEQPT-PBWORK) alarm indicates a failure in the main payload bus between the Slot 8 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card, the reporting traffic card, or the backplane.

Note If all traffic cards show CTNEEQPT-PBWORK alarm, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 for the active TCC2 card and then complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-219 for the TCC2 card. Do not physically reseat an active TCC2 card; it disrupts traffic.

Note This alarm automatically raises and clears when the Slot 10 XC10G cross-connect card is reseated.

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 CTNEQPT-PBWORK Alarm

Step 1 Complete the "Side Switch the Active and Standby XC10G Cross-Connect cards" procedure on page 2-216 for the active XC10G cross-connect card.

Note After the active cross-connect goes into standby, the original standby slot becomes active. The active card ACT/SBY LED becomes green.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the standby cross-connect card.

Note The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

Step 5 If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216. If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

Step 6 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 7 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 8 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 9 If you switched traffic, complete the "Clear a Protection Group External Switching Command" procedure on page 2-216.

Step 10 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 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 2-219 for the reporting traffic card.

Step 12 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.58 DATAFLT

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Software Data Integrity Fault (DATAFLT) alarm occurs when the TCC2 exceeds its flash memory capacity.

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

Clear the DATAFLT Alarm

Step 1 Complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.59 DBOSYNC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The standby Database Out Of Synchronization (DBOSYNC) alarm occurs when the standby TCC2 "To be Active" database does not synchronize with the active database on the active TCC2.

Caution If you reset the active TCC2 card while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TCC2 database. Complete the "Back Up the Database" procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

a. In node view, click the **Provisioning > General > General** tabs.

b. In the Description field, make a small change such as adding a period to the existing entry.

The change causes a database write but does not affect the node state. The write could take up to a minute.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.60 DSP-COMM-FAIL

- Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The digital signal processor (DSP) Communication Failure alarm (DSP-COMM-FAIL) indicates that there is a communications failure between an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card microprocessor and the on-board DSP chip that controls the trunk (DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card microprocessor attempts to restore communication with the DSP chip until the alarm is cleared.

If the alarm is raised for an extended period, the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card raises the "DSP-FAIL" alarm on page 2-63, and could affect traffic.

Note DSP-COMM-FAIL is informational. The alarm does not require troubleshooting.

2.7.61 DSP-FAIL

- Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The DSP Failure (DSP-FAIL) alarm indicates that a "DSP-COMM-FAIL" alarm on page 2-63 has persisted for an extended period on an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the reporting MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.62 DS3-MISM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Frame Format Mismatch (DS3-MISM) condition indicates a frame format mismatch on a signal transiting the DS3XM-6 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type is set to C Bit for a DS3XM-6 card, and the incoming signal's frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting DS3XM-6 card.

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

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

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

Step 5 Click **Apply**.

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

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

Step 7 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.63 DUP-IPADDR

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area. When this happens, TC no longer reliably connects to either node. Depending on how the packets are routed, CTC may connect to either node (having the same IP address). If CTC has connected to both nodes before they shared the same address, it has two distinct NodeModel instances (keyed by the node ID portion of the MAC address).

Clear the DUP-IDADDR Alarm

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 In the IP Address field, change the IP address to a unique number.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.64 DUP-NODENAME

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate Node Name (DUP-NODENAME) alarm indicates that the alarmed node’s alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

Step 1 In node view, click the **Provisioning > General > General** tabs.

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.65 EHIBATVG

- Major (MJ), Service-Affecting (NSA)
- Logical Object: PWR

The Extreme High Voltage Battery (EHIBATVG) alarm occurs in a –48 VDC environment when a battery lead's input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide*.)

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.66 ELWBATVG

- Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Extreme Low Voltage Battery (ELWBATVG) alarm occurs in a –48 VDC environment when a battery lead's input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide*.)

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.67 EOC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The SONET Data Communications Channel (DCC) Termination Failure alarm occurs when the ONS 15454 loses its data communications channel. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its OC-3 section overhead.

The SDCCs consist of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15454 uses the DCC on the SONET section layer to communicate network management information.

Warning **On the 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC Alarm

Step 1 If the "LOS (DS1)" alarm on page 2-128 is also reported, complete the "Clear the LOS (DS1) Alarm" procedure on page 2-128.

Step 2 If the alarm does not clear on the reporting node, verify the physical connections between the cards and 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 (IS) ports by checking that the ACT LED on each OC-N card is illuminated.

Step 4 If the ACT LEDs on OC-N cards are illuminated, complete the "Verify or Create Node DCC Terminations" procedure on page 2-214 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the port is active and in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

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

c. 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 click **IS** from the pull-down menu. Click **Apply**.

Step 7 For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations.

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

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

Step 8 If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. See the "OC-N Card Transmit and Receive Levels" section on page 1-102 non-DWDM card levels and see the *Cisco ONS 15454 Reference Manua*l for DWDM card levels.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the "Install the Fiber-Optic Cables" procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2 switches control to the standby TCC2. If the alarm clears when the ONS 15454 switches to the standby TCC2, the user can assume that the original active TCC2 is the cause of the alarm.

Step 11 If the TCC2 reset does not clear the alarm, delete the problematic DCC termination:

a. From card view, click **View > Go to Previous View** if you have not already done so.

a. Click the **Provisioning > DCC/GCC/OSC** tabs.

b. Highlight the problematic DCC termination.

c. Click **Delete**.

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

Step 12 Recreate the DCC termination. Refer to the *Cisco ONS 15454 Procedure Guide* for instructions.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.68 EOC-L

- Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: OCN, TRUNK

The Line DCC Termination Failure alarm occurs when the ONS 15454 loses its line data communications channel. For example, the OSCM card can raise this alarm on its OC-3 line overhead.

The LDCCs are nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS 15454 uses the LDCCs on the SONET line layer to communicate network management information.

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

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Note If a circuit shows an incomplete state when the EOC alarm is raised, it occurs when the logical circuit is in place. The circuit will be able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-67.

Step 2 If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.69 EQPT

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AIE, EQPT

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

If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "BKUPMEMP" section on page 2-42. The BKUPMEMP procedure also clears 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 at the lower-right outside edge of the shelf assembly.

Clear the EQPT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 3 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 4 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

⚠ **Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.70 EQPT-MISS

- Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Replaceable Equipment or Unit Missing (EQPT-MISS) alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted or that the ribbon cable connecting the AIP to the system board may be bad.

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

Clear the EQPT-MISS Alarm

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

Step 2 If the fan-tray assembly is present, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-220.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the "Install the Fan-Tray Assembly," procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 4 If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.71 ERFI-P-CONN

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The three-bit enhanced remote failure indication (ERFI) Path Connectivity condition (ERFI-P-CONN) is triggered on DS-1, DS-3, and VT circuits when the "UNEQ-P" alarm on page 2-204 and the "TIM-P" alarm on page 2-199 are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-204. This should clear the ERFI condition.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.72 ERFI-P-PAYLD

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The ERFI Path Payload (ERFI-P-PAYLD) condition is triggered on DS-1, DS-3, and VT circuits when the "PLM-P" alarm on page 2-167 alarm is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

Step 1 Complete the "Clear the PLM-P Alarm" procedure on page 2-167. This should clear the ERFI condition.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.73 ERFI-P-SRVR

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The ERFI Path Server (ERFI-:P-SRVR) condition is triggered on DS-1, DS-3, and VT circuits when the "AIS-P" alarm on page 2-22 or the "LOP-P" alarm on page 2-125 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-125. This should clear the ERFI condition.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.74 ERROR-CONFIG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Error in Startup Configuration (ERROR-CONFIG) alarm applies to the ML-Series Ethernet (traffic) cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.

For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

Clear the ERROR-CONFIG Alarm

Step 1 If you have a different type of ML-Series card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

Step 2 Upload the configuration file to the TCC2:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location in the Open dialog box.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218.

Step 4 If the alarm does not clear or if your configuration file was correct according to the installed card, start an IOS CLI for the card:

a. Right click the ML-Series card graphic in node view.

b. Choose **Open IOS Connection** from the shortcut menu.

Note Open IOS Connection is not available unless the ML-Series card is physically installed in the shelf.

Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* to correct the errored configuration file line.

Step 5 Execute the CLI command **copy run start**. The command copies the new card configuration into the database and clears the alarm.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.75 ETH-LINKLOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Rear Panel Ethernet Link Removed (ETH-LINKLOSS) condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Clear the ETH-LINKLOSS Condition

Step 1 To clear this alarm, reconnect the backplane LAN cable. Refer to the *Cisco ONS 15454 Procedure Guide* for instructions to install this cable.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.76 E-W-MISMATCH

- Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

A Procedural Error Misconnect East/West Direction (E-W-MISMATCH) alarm occurs when nodes in a ring have an east slot misconnected to another east slot or a west slot misconnected to another west slot. In most cases, the user did not connect the fibers correctly or the ring provisioning plan was flawed. You can physically reconnect the cable to the correct slots to clear the E-W-MISMATCH alarm. Alternately, you can delete and recreate the span in CTC to change the west line and east line designations. The CTC method clears the alarm, but could change the traditional east-west node connection pattern of the ring.

Note The E-W-MISMATCH alarm also appears during the initial set up of a ring with its East-West slots configured correctly. If the alarm appears during the initial setup, the alarm clears itself shortly after the ring setup is complete.

Note The lower numbered slot at a node is traditionally labeled as the west slot and the higher numbered slot is labeled as the east slot. For example, Slot 6 is west and Slot 12 is east.

Note The physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slots as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

Clear the E-W-MISMATCH Alarm with a Physical Switch

Step 1 Diagram the ring setup, including nodes and spans, on a piece of paper or white board.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Label each of the nodes on the diagram with the same name that appears on the network map.

Step 4 Right-click each span to reveal the node name/slot/port for each end of the span.

Step 5 Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 - Node2/Slot6/Port1 (2F BLSR OC48, ring name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/ Port 1.

Step 6 Repeat Steps 4 and 5 for each span on your diagram.

Step 7 Label the highest slot at each node east and the lowest slot at each node west.

Step 8 Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about configuring the system.

Step 9 If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.

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

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

Step 10 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Clear the E-W-MISMATCH Alarm in CTC

Step 1 Log into the misconnected node. A misconnected node has both ring fibers connecting it to its neighbor nodes misconnected.

Step 2 Click the **Maintenance > BLSR** tabs.

Step 3 From the row of information for the fiber span, complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213 to identify the node ID, ring name, and the slot and port in the East Line list and West Line columns. Record the above information.

Step 4 Click **View > Go to Network View**.

Step 5 Delete and recreate the BLSR:

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

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

c. Click **Create BLSR**.

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

e. Click **Finish** in the BLSR Creation window.

Step 6 Display node view and click the **Maintenance > BLSR** tabs.

Step 7 Change the West Line pull-down menu to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line pull-down menu to the slot you recorded for the West Line in Step 3.

Step 9 Click **OK**.

Step 10 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.77 EXCCOL

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Excess Collisions on the LAN (EXCCOL) alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2 card. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC2 card for excess collisions. You may need to contact the system administrator of the network management LAN to accomplish the following steps.

Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the TCC2 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 TCC2 card and the network management LAN.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.78 EXERCISE-RING-FAIL

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

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

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

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-123, the "LOS (OCN)" alarm on page 2-132, or BLSR alarms.

Step 2 Reissue the Exercise Ring command:

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

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

c. Select **Exercise Ring** in the pull-down menu.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.79 EXERCISE-SPAN-FAIL

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

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

Note If the exercise command gets rejected due to the existence of a higher priority condition in the span or ring, EXERCISE-SPAN-FAIL is not reported.

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-123, the "LOS (OCN)" alarm on page 2-132, or a BLSR alarm.

Step 2 Reissue the Exercise Span command:

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

b. Determine whether the card you would like to exercise is the west card or the east card.

c. Click the row of the affected span under the East Switch or West Switch column.

d. Select **Exercise Span** in the pull-down menu.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.80 EXT

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: ENVALRM

A Failure Detected External to the NE (EXT) alarm occurs because an environmental alarm is present. For example, a door could be open or flooding may have occurred.

Clear the EXT Alarm

Step 1 In node view, double-click the AIC or AIC-I card to display the card view.

Step 2 Click the **Maintenance** tab to gather further information about the EXT alarm.

Step 3 Perform your standard operating procedure for the environmental condition.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.81 EXTRA-TRAF-PREEMPT

- Major (MJ), Service Affecting (SA)
- Logical Object: OCN

An Extra Traffic Preempted (EXT-TRAF-PREEMPT) alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Clear the EXTRA-TRAF-PREEMPT Alarm

Step 1 Verify that the protection switch has occurred by checking the Conditions tab.

Step 2 If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm occurred on a four-fiber BLSR and the span switch occurred on this OC-N, clear the span switch on the working system.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.82 FAILTOSW

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, TRUNK

The Failure to Switch to Protection (FAILTOSW) condition occurs when a working electrical (traffic) card cannot switch to the protect card in a 1:N, Y-cable, or splitter protection group because another working electrical card with a higher-priority alarm has switched to the protect card.

Clear the FAILTOSW Condition

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

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

Step 2 If the condition does not clear, replace the working electrical (traffic) card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 2-219. This card is the working electrical card using the 1:N card protection and not reporting FAILTOSW.

Replacing the working electrical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.83 FAILTOSW-PATH

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The FAILTOSW Path (FAILTOSW-PATH) condition occurs when the working path does not switch to the protection path on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection card or a lockout set on one of the path protection 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 at the lower-right outside edge of the shelf assembly.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Step 1 Look up and clear the higher priority alarm. Clearing this condition frees the standby card and clears the FAILTOSW-PATH condition.

Step 2 If the condition does not clear, replace the active OC-N card that is reporting the higher priority alarm. Complete the "Physically Replace a Card" procedure on page 2-219. Replacing the active OC-N card that is reporting the higher priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower priority alarm and the FAILTOSW-PATH condition.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.84 FAILTOSWR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The FAILTOSW Ring (FAILTOSW-RING) condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears when one of the following situations occurs:

- a physical card pull of the active TCC card (done under TAC supervision);
- a node power cycle;
- a higher priority event such as an external switch command;

- the next ring switch succeeds;
- or, the cause of the APS switch (such as the "SD (DS1, DS3)" condition on page 2-178 or the "SF (DS1, DS3)" condition on page 2-182) 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 could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.**

Clear the FAILTOSWR Condition in a Four-Fiber BLSR Configuration

Step 1 Perform the EXERCISE RING command on the reporting card:

- **a.** Click the **Maintenance > BLSR** tabs.
- **b.** Click the row of the affected ring under the West Switch column.
- **c.** Select **Exercise Ring** in the pull-down menu.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

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

Step 4 If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node.

Step 5 Click the **Maintenance > BLSR** tabs.

Step 6 Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards and ports and port are active and in service:

- **a.** Confirm that the OC-N card shows a green LED in CTC or on the physical card.

  A green LED indicates an active card. An amber LED indicates a standby card.
- **b.** Double-click the card in CTC to display the card view.
- **c.** Click the **Provisioning > Line** tabs.
- **d.** Verify that the State column lists the port as IS.
- **e.** If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 7 If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

Step 8 If fiber continuity to the ports is okay, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Caution Using an optical test set disrupts service on the optical (traffic) card. It could be necessary to manually switch traffic carrying circuits over to a protection path.

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure 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 "OC-N Card Transmit and Receive Levels" section on page 1-102 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 13 If the condition does not clear after you replace the BLSR cards on the node one by one, repeat Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.85 FAILTOSWS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The FAILTOSW Span (FAILTOSWS) condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following situations occurs:

- a physical card pull of the active TCC card (done under TAC supervision);
- a node power cycle;
- a higher priority event such as an external switch command occurs;
- the next span switch succeeds;
- or, the cause of the APS switch (such as the "SD (DS1, DS3)" condition on page 2-178 or the "SF (DS1, DS3)" condition on page 2-182) clears.

Clear the FAILTOSWS Condition

Step 1 Perform the EXERCISE SPAN command on the reporting card:

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

b. Determine whether the card you would like to exercise is the west card or the east card.

c. Click the row of the affected span under the East Switch or West Switch column.

d. Select **Exercise Span** in the pull-down menu.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

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

Step 4 If clearing other alarms does not clear the FAILTOSWS condition, log into the near-end node and click the **Maintenance > BLSR** tabs.

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

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber 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 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 the ports is okay, verify that the correct port is in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber 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 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.

Caution Using an optical test set disrupts service on the optical (traffic) card. It could be necessary to manually switch traffic carrying circuits over to a protection path.

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure 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 "OC-N Card Transmit and Receive Levels" section on page 1-102 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 13 If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.86 FAN

- Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Fan Failure (FAN) alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range. The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the ONS 15454. However, even with five working fans, the fan-tray assembly could need replacement because a sixth working fan is required for extra protection against overheating.

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

Clear the FAN Alarm

Step 1 Determine whether the air filter to see whether it needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 3-5.

Step 2 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-220.

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 3-10.

Step 4 If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.87 FANDEGRADE

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FAN

The Partial Fan Failure Speed Control Degradation (FANDEGRADE) alarm occurs if fan speed for one of the fans in the fan-tray assembly falls under 500 RPM when read by a tachometry counter.

Clear the FANDEGRADE Alarm

Step 1 Complete the "Clear the FAN Alarm" procedure on page 2-83.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.88 FE-AIS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End AIS (FE-AIS) condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the "LOS (OCN)" alarm on page 2-132).

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.89 FEC-MISM

- Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The forward error correction (FEC) Mismatch alarm (FEC-MISM) occurs if one end of a span using MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G cards is configured to use FEC and the other is not. FEC-MISM is related to ITU-T G.709 and is only raised against a trunk port.

Clear the FEC-MISM Alarm

Step 1 Double-click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card.

Step 2 Click the **Provisioning > OTN > OTN Lines** tab.

Step 3 Check the FEC column check box.

Step 4 Verify that the far-end card is configured the same way by repeating Step 1 through Step 3.

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

2.7.90 FE-DS1-MULTLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Multiple DS-1 LOS Detected (FE-DS1-MULTLOS) condition occurs when multiple DS-1 signals are lost on a far-end DS-1 card. The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.91 FE-DS1-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Non-Service Affecting (FE-DS1-NSA) condition occurs when a far-end DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-NSA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.92 FE-DS1-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Service Affecting (FE-DS1-SA) condition occurs when there is a far-end equipment failure on a DS-1 card that affects service because traffic is unable to switch to the protect port.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.93 FE-DS1-SNGLLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Single DS-1 LOS (FE-DS1-SNGLLOS) condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment. Signal loss also causes the "LOS (OCN)" alarm on page 2-132. The prefix FE in an alarm or 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SNGLLOS Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.94 FE-DS3-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-3 Equipment Failure Non-Service Affecting (FE-DS3-NSA) 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 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-NSA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.95 FE-DS3-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-3 Equipment Failure Service Affecting (FE-DS3-SA) condition occurs when there is a far-end equipment failure on a DS-3 card that affects service because traffic is unable to switch to the protect port.

The prefix FE in an alarm or 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-SA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.96 FE-EQPT-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End Common Equipment Failure (FE-EQPT-NSA) condition occurs when a non-service-affecting equipment failure is detected on the far-end DS-3 equipment. The prefix FE occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-EQPT-NSA alarm. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

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 FE-EQPT-NSA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.97 FE-FRCDWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Working Facility Forced to Switch to Protection (FE-FRCDWKSWPR-RING) condition occurs from a far-end node when a ring is forced from working to protect using the FORCE RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm. See the "Clear a BLSR External Switching Command" procedure on page 2-215 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.98 FE-FRCDWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span (FE-FRCDWKSWPR-SPAN) condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the FORCE SPAN command.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-FRCDWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm. See the "Clear a BLSR External Switching Command" procedure on page 2-215 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.99 FE-IDLE

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End Idle (FE-IDLE) condition occurs when a far-end node detects an idle DS-3 signal.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-IDLE condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Clear the FE-IDLE Condition

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

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

Step 3 Clear the main alarm. Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.100 FE-LOCKOUTOFPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far-End Lock Out of Protection Span (FE-LOCKOUTOFPR-SPAN) condition occurs when a BSLR span is locked out of the protection system from a far-end node using the Lockout Protect Span command.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOCKOUTOFPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Ensure there is no lockout set. See the "Clear a BLSR External Switching Command" procedure on page 2-215 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.101 FE-LOF

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOF (FE-LOF) condition occurs when a far-end node reports the "LOF (DS3)" alarm on page 2-122.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-LOF condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOF Condition

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

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

Step 3 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-121. It also applies to FE-LOF.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.102 FE-LOS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOS (FE-LOS) condition occurs when a far-end node reports the "LOS (DS3)" alarm on page 2-129.

The prefix FE occurs when 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOS Condition

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

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

Step 3 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-128.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.103 FE-MANWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Manual Switch of Working Facility to Protect (FEMANWKSWPR-RING) condition occurs when a BLSR working ring is switched from working to protect at a far-end node using the MANUAL RING command.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.104 FE-MANWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect (FE-MANWKSWPR-SPAN) condition occurs when a BLSR span is switched from working to protect at the far-end node using the MANUAL SPAN command.

The prefix FE 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. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.105 FEPRLF

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Protection Line Failure (FEPRLF) alarm occurs when an APS channel "SF (DS1, DS3)" condition on page 2-182 occurs on the protect card coming into the node.

Note The FEPRLF alarm occurs only on the ONS 15454 when bidirectional protection is used on optical (traffic) cards in a 1+1 configuration or four-fiber BLSR configuration.

Clear the FEPRLF Alarm on a Four-Fiber BLSR

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.106 FIBERTEMP-DEG

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

The Fiber Temperature Degrade (FIBERTEMP-DEG) alarm occurs when a DWDM card internal heater-control circuit fails. Degraded temperature can cause some signal drift. The card should be replaced at the next opportunity.

Clear the FIBERTEMP-DEG Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-219 at the next opportunity.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.107 FORCED-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Force Switch Request (FORCED-REQ) 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 the condition if you want the Force switch to remain.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.108 FORCED-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Force Switch Request Ring (FORCED-REQ-RING) condition applies to optical trunk cards when the FORCE RING command is applied to two-fiber and four-fiber BLSRs to move traffic from working to protect.

Clear the FORCED-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.109 FORCED-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Force Switch Request Span (FORCED-REQ-SPAN) condition applies to optical trunk cards in four-fiber BLSRs when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.110 FRCDSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Force Switch to Internal Timing (FRCDSWTOINT) condition occurs when the user issues a Force command to switch to an internal timing source.

Note FRCDSWTOINT is an informational condition. It does not require troubleshooting.

2.7.111 FRCDSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source (FRCDSWTOPRI) condition occurs when the user issues a Force command to switch to the primary timing source.

Note FRCDSWTOPRI is an informational condition. It does not require troubleshooting.

2.7.112 FRCDSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source (FRCDSWTOSEC) condition occurs when the user issues a Force command to switch to the second timing source.

Note FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

2.7.113 FRCDSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source (FRCDSWTOTHIRD) condition occurs when the user issues a Force command to switch to the third timing source.

Note FRCDSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.7.114 FRNGSYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Free Running Synchronization Mode (FRNGSYNC) 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 building integrated timing supply (BITS) timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 relying on an internal clock.

Note If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Alarm

Step 1 If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the *Cisco ONS 15454 Reference Manual* for more information about timing.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-195 and the "SYNCSEC" alarm on page 2-196.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.115 FSTSYNC

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

A Fast Start Synchronization Mode (FSTSYNC) alarm occurs 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note FSTSYNC is an informational alarm. It does not require troubleshooting.

2.7.116 FULLPASSTHR-BI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Bidirectional Full Pass-Through Active (FULLPASSTHR-BI) condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic and there is a change in the receive K byte from No Request.

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.117 GAIN-HDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Optical Amplifier Gain Degrade High (GAIN-HDEG) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card keeps the gain level from maintaining the set-point.

Clear the GAIN-HDEG Alarm

Step 1 This alarm does not immediately affect traffic, but eventually to clear the alarm you will need to complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.118 GAIN-HFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Optical Amplifier Gain High Fail (GAIN-HFAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem causes the card to fail by forcing the gain level to consistently exceed the set-point.

Clear the GAIN-HFAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.119 GAIN-LDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Optical Amplifier Gain Degrade Low (GAIN-LDEG) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card keeps the gain level from reaching the set-point.

Clear the GAIN-LDEG Alarm

Step 1 This alarm does not immediately affect traffic. But eventually, to clear the alarm, you will need to complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.120 GAIN-LFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Optical Amplifier Gain Fail Low (GAIN-LFAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card causes the card to fail by preventing the gain level from reaching the set-point.

Clear the GAIN-LFAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.121 GCC-EOC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Gnu C Compiler (GCC) Embedded Operation Channel Failure (GCC-EOC) alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. The GCC-EOC is raised when the channel cannot operate.

Clear the GCC-EOC Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-67.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.122 GE-OOSYNC

- Critical (CR), Service-Affecting (SA)
- Logical Objects: CLIENT, TRUNK

The Gigabit Ethernet Out of Synchronization (GE-OOSYNC) alarm applies to TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G cards when the Gigabit Ethernet signal is out of synchronization and is very similar to the SONET LOS alarm. This alarm can occur when you try to input a SONET signal to the TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card. A signal is present, so there is no CARLOSS alarm, but it is not correctly formatted for the card and so it raises the GE-OOSYNC alarm.

Clear the GE-OOSYNC Alarm

Step 1 Ensure that the incoming signal is provisioned with the correct physical-layer protocol.

Step 2 Ensure that the line is provisioned with the correct line speed (10 Gbps).

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.123 HIBATVG

- Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The High Voltage Battery (HI-BATVG) alarm occurs in a –48 VDC environment when a battery lead's input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide*.)

Clear the HIBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.124 HI-LASERBIAS

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Equipment High Transmit Laser Bias Current (HI-LASERBIAS) alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer's maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser's usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Clear the LASEREOL Alarm" procedure on page 2-117. Replacement is not urgent and can be scheduled during a maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.125 HI-RXPOWER

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Equipment High Receive Power (HI-RXPOWER) alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Step 1 Find out whether gain (the amplification power) of any amplifiers has been changed. The change also causes channel power to need adjustment.

Step 2 Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.

Note If the card is part of an amplified dense wavelength division multiplexing system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

Step 4 If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at once and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dB.

Step 5 If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance according to standard practice.

Step 6 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Card" procedure on page 2-219. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 8 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.126 HITEMP

- Critical (CR), Service-Affecting (SA) for NE
- Minor (MN), Non-Service Affecting (NSA) for EQPT
- Logical Objects: EQPT, NE

The High Temperature (HITEMP) alarm occurs when the temperature of the ONS 15454 is above 122 degrees F (50 degrees C).

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 HITEMP Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-1 on page 2-35).

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

Step 3 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454.

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, determine whether the air filter needs replacement. Refer to the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 3-5.

Step 6 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-220.

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 3-10.

Step 8 If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC 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.

2.7.127 HI-TXPOWER

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Equipment High Transmit Power (HI-TXPOWER) alarm is an indicator on the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Clear the HI-TXPOWER Alarm

Step 1 In node view, display the card view for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card.

Step 2 Click the **Provisioning > Optical Thresholds** tabs.

Step 3 Decrease (change toward the negative direction) the TX Power High column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.128 HLDOVRSYNC

- Major (MJ), Service-Affecting (SA)
- Logical Object: NE-SREF

The Holdover Synchronization Mode (HLDOVRSYNC) 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 ONS 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.

Clear the HLDOVRSYNC Alarm

Step 1 Clear additional alarms that relate to timing, such as:

- FRNGSYNC, page 2-96
- FSTSYNC, page 2-97
- HLDOVRSYNC, page 2-104
- LOF (BITS), page 2-120

- LOS (BITS), page 2-127
- MANSWTOINT, page 2-146
- MANSWTOPRI, page 2-146
- MANSWTOSEC, page 2-146
- MANSWTOTHIRD, page 2-147
- SWTOPRI, page 2-194
- SWTOSEC, page 2-194
- SWTOTHIRD, page 2-194
- SYNC-FREQ, page 2-195
- SYNCPRI, page 2-195
- SYNCSEC, page 2-196
- SYNCTHIRD, page 2-197

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.129 I-HITEMP

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: NE

The Industrial High Temperature (I-HITEMP) alarm occurs when the temperature of the ONS 15454 is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Step 1 Complete the "Clear the HITEMP Alarm" procedure on page 2-103.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447) in order to report a service-affecting problem.

2.7.130 IMPROPRMVL

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Improper Removal (IMPROPRMVL) alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node.

Caution Do not remove a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot.

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.

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

Note It can take up to 30 minutes for software to be updated on a standby TCC2 card.

Clear the IMPROPRMVL Alarm

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

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

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

Step 3 If any ports on the card are in service, place them out of service (OOS):

Caution Before placing a port out of service (OOS), ensure that no live traffic is present.

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

b. Click the **Provisioning > Line** tab.

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

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

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-217.

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

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

a. Click **View > Go to Previous View** to return to node view.

b. If you are already in node view, click the **Provisioning > Protection** tabs.

c. Click the protection group of the reporting card.

d. Click **Delete**.

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

a. Click the **Provisioning > DCC/GCC/OSC** tabs.

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

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

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

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

b. Under NE Reference, click the pull-down menu for **Ref-1**.

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

d. Click **Apply**.

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

Step 9 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.131 INC-GFP-OUTOFFRAME

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Out of Frame Detected by general framing procedure (GFP) Receiver condition (INC-GFP-OUTOFFRAME) can be caused by anything that prevents GFP communication across the SONET link, such as typical errors (AIS-P, LOP-P, PLM-P, or UNEQ-P); virtual concatenation (VCAT) member errors (SQM); and VCAT group errors. If a VCAT is present, the VCG-DOWN, LOA, or LOM alarms are generated if any of the normal SONET errors are generated.

Clear the INC-GFP-OUTOFFRAME Condition

Step 1 Resolve any normal SONET errors also occurring on the errored circuit. Refer to the appropriate sections for any alarms that are present:

- "AIS-P" alarm on page 2-22
- "LOP-P" alarm on page 2-125
- "PLM-P" alarm on page 2-167
- "UNEQ-P" alarm on page 2-204

Step 1 If the errored circuit is a VCAT circuit and no other SONET alarms are occurring, look for and clear any VCAT alarms. Refer to the appropriate sections for any alarms that are present:

- "SQM" alarm on page 2-188
- "VCG-DEG" alarm on page 2-206

- "VCG-DOWN" alarm on page 2-207.

Step 2 If a protection switch occurred on the STS carrying the circuit, the INC-GFP-OUTOFFRAME condition will clear when the working circuit is restored and able to carry traffic. For general information about protection switches, refer to the *Cisco ONS 15454 Procedure Guide* and the *Cisco ONS 15454 Reference Manual*. To clear a protection switch (if the working card or port is available for service), complete the "Clear a Protection Group External Switching Command" procedure on page 2-216.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.132 INC-GFP-SIGLOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Client Signal Loss Frames Detected by GFP Server (INC-GFP-SIGLOSS) condition occurs when the upstream GFP transmitter has no signal from its fibre channel link. This condition occurs in conjunction with the "INC-SIGLOSS" alarm on page 2-109.

Clear the INC-GFP-SIGLOSS Condition

Step 1 Check the fibre channel data port connection at the remote fibre channel card port on the other end of the SONET link.

Step 2 Verify fiber continuity to the port.

Step 3 Check the physical port LED on the fibre channel card. The port LED looks clear (that is, not lit green) if the link is not connected.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.133 INC-GFP-SYNCLOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Client Synchronization Loss Frames Detected by GFP Receiver (INC-GFP-SYNCLOSS) condition occurs when the upstream GFP transmitter has no synchronization from its fibre channel link. This alarm is raised in conjunction with the "INC-SYNCLOSS" alarm on page 2-110.

Errors in synchronization can be caused if the fibre channel link is set for a speed that is not compatible with the attached equipment or if the port has an GBIC connector that is incompatible with the link speed. When the GBIC does not support the line speed, the PORT-MISMATCH alarm could also be raised.

Clear the INC-GFP-SYNCLOSS Condition

Step 1 For the errored circuit, log into both ends of the SONET link where the fibre channel connection is present, and ensure that the fibre channel link is set to run at a compatible speed for the attached equipment (for example, 1 Gbps or 2 Gbps):

a. Double-click the fibre channel card to display the card view.

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

c. Under the Port Rate column, choose a speed that is compatible with the attached fibre channel equipment (either 1 Gbps or 2 Gbps).

Note You must choose the same line rate on both ends of the fibre channel link.

d. Click **Apply**.

Step 2 If the line rate is correctly set on both ends of the circuit, the remote card could have an incompatible GBIC for the link speed.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.134 INC-ISD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Idle (INC-ISD) condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OO-MT state. It is resolved when the OOS state ends.

Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.7.135 INC-SIGLOSS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Incoming Signal Loss on the Fibre Channel Interface (INC-SIGLOSS) alarm is raised when there is a signal loss at the local fibre channel port. (The "INC-GFP-SIGLOSS" alarm on page 2-108 is raised at the far-end port in conjunction with this alarm.)

Clear the INC-SIGLOSS Alarm

Step 1 Check the fibre channel data port connection at the near-end fibre channel card port of the SONET link.

Step 2 Verify fiber continuity to the port.

Step 3 Check the physical port LED on the fibre channel card. The port LED looks clear (that is, not lit green) if the link is not connected.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.136 INC-SYNCLOSS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Incoming Synchronization Loss on the Fibre Channel Interface (INC-SYNCLOSS) alarm is raised when there is a synchronization error at the local fibre channel port. (The "INC-GFP-SYNCLOSS" alarm on page 2-108 is raised at the far-end port in conjunction with this alarm.)

Clear the INC-SYNCLOSS Alarm

Step 1 Complete the "Clear the INC-GFP-SYNCLOSS Condition" procedure on page 2-109.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.137 INHSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment (INHSWPR) condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a 1:N protection scheme, traffic can be switched between working cards when the switch to protect is disabled.

Clear the INHSWPR Condition

Step 1 Complete the "Clear a Protection Group External Switching Command" procedure on page 2-216.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.138 INHSWWKG

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment (INHSWWKG) condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a 1:N protection scheme, traffic can be switched between protect cards when the switch to working is disabled.

Clear the INHSWWKG Condition

Step 1 Complete the "Clear a Protection Group External Switching Command" procedure on page 2-216.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.139 INTRUSION-PSWD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Security Intrusion Incorrect Password (INTRUSION-PSWD) condition occurs after a user attempts a settable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a settable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if lockout is permanent.

Clear the INTRUSION-PSWD Condition

Step 1 In node view, click the **Provisioning > Security** tabs.

Step 2 Click the **Clear Security Intrusion Password Alarm** button.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.140 INVMACADR

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AIP

The Equipment Failure Invalid MAC Address (INVMACADR) alarm occurs when the ONS 15454 Media Access Control layer address (MAC address) is invalid. Each ONS 15454 has a unique, permanently assigned MAC address that resides on an Alarm Interface Panel (AIP) EEPROM. The TCC2 card reads the address value from the AIP chip during boot-up and keeps this value in its Synchronous Dynamic RAM (SDRAM). Under normal circumstances, the read-only MAC address can be viewed in the Provisioning/Network tab in the Cisco Transport Controller (CTC).

The Cisco ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you will see an incomplete circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit's end-to-end information.

An invalid MAC address can by caused when:

- There is a read error from the AIP during bootup; in this case, the reading TCC2 uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2 cards that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad

Clear the INVMACADR Alarm

Step 1 Check for any outstanding alarms that were raised against the active and standby TCC2 and resolve them.

Step 2 Determine whether the LCD display on the fan tray is blank or if the text is garbled. If so, proceed to Step 8 (Figure 2-1 on page 2-35). If not, continue with Step 3.

Step 3 At the earliest maintenance window, reset the standby TCC2:

Note The reset will take approximately five minutes. Do not perform any other step until the reset is complete.

a. Log into a node on the network. If you are already logged in, continue with Step b.

b. Identify the active TCC2 card.

If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.

c. Right-click the standby TCC2 card in CTC.

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

e. Click **Yes** at the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

f. Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

g. Double-click the node and ensure that the reset TCC2 card is still in standby mode and that the other TCC2 card is active.

If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.

h. Ensure that no new alarms appear in the Alarms window in CTC that are associated with this reset.

If the standby TCC2 fails to boot into standby mode and reloads continuously, the alarm interface panel (AIP) is likely defective. In this case, the standby TCC2 is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2 reloads until it reads the EEPROM. Proceed to Step 8.

Step 4 If the standby TCC2 rebooted successfully into standby mode, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Resetting the active TCC2 causes the standby TCC2 to become active. The standby TCC2 keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

Step 5 After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

Step 6 Complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 again to place the standby TCC2 back into active mode.

After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2 resets, this indicates that the AIP is probably defective. Proceed to Step 8.

If the INVMACADR was raised during one TCC2 reset and cleared during the other, the TCC2 that was active during the alarm raise needs to be replaced. Continue with Step 7.

Step 7 If the faulty TCC2 is currently in standby mode, complete the "Physically Replace a Card" procedure on page 2-219 for this card. If the faulty TCC2 card is currently active, during the next available maintenance window complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217 and then complete the "Physically Replace a Card" procedure on page 2-219.

Note If the replacement TCC2 is loaded with a different software version from the current TCC2 card, the card bootup may take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2 version software is copied to the new standby card.

Step 8 Open a case with the Cisco Technical Assistance Center (1-800-553-2447) for assistance with determining the node's previous MAC address.

Step 9 Replace the ribbon cable between the system board and the AIP with a known-good cable.

Step 10 If the alarm persists, complete the "Replace the Alarm Interface Panel" procedure on page 3-12.

Step 11 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1 800 553-2447).

2.7.141 IOSCFGCOPY

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The IOS Configuration Copy in Progress (IOSCFGCOPY) condition occurs on ML-Series Ethernet cards when an IOS startup configuration file is being uploaded or downloaded to or from an ML-Series card. (This condition is very similar to the "SFTWDOWN" condition on page 2-183 but it applies to ML-Series Ethernet cards rather than to the TCC2.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the "NO-CONFIG" condition on page 2-152 could be raised.)

Note IOSCFGCOPY is an informational condition.

2.7.142 KB-PASSTHR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The K Bytes Pass Through Active (KB-PASSTHR) condition occurs on a nonswitching node in a BLSR when the protect channels on the node are not active and the node is in K Byte Pass-Through State.

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.143 KBYTE-APS-CHANNEL-FAILURE

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Channel Failure (KBYTE-APS-CHANNEL-FAILURE) alarm is raised when there a span provisioned for different APS channels on each side. For instance, the alarm is raised if K3 is selected on one end and F1, E2, or Z2 is selected on the other end.

This alarm is also raised during checksum failure occurs if the K1 and K2 bytes are overwritten by test equipment. It is not raised in bidirectional full pass-through or K Byte pass-through states. The alarm is overridden by AIS-P, LOF, LOS, or SF-BER alarms.

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

Step 1 The alarm most frequently is raised due to mismatched span provisioning. In this case, reprovision one side of the span with the same parameters. To do this, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2 card. Complete the "Side Switch the Active and Standby XC10G Cross-Connect cards" alarm on page 2-216 to allow the CTC to resolve the issue.

Step 3 If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.144 LAN-POL-REV

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The LAN Connection Polarity Reversed (LAN-POL-REV) condition is not raised in shelves that contain TCC2 cards. It is raised by the TCC+ card during software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The TCC+ automatically compensates for this reversal, but LAN-POL-REV stays active.

Clear the LAN-POL-REV Condition

Step 1 Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.145 LASER-APR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Auto Power Reduction (LASER-APR) condition occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when the amplifier works at a reduced power level for a fixed period during the automatic restart. The condition raises and clears within about 10 seconds.

Note LASER-APR is information condition only and does not require troubleshooting.

2.7.146 LASERBIAS-DEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Laser Bias Degrade (LASERBIAS-DEG) alarm occurs on DWDM amplifiers (OPT-BST and OPT-PRE) and optical service channel cards (OSCM and OSC-CSM) if the card laser crosses the laser bias degrade threshold. This degradation occurs due to laser aging.

Clear the LASERBIAS-DEG Alarm

Step 1 This alarm does not immediately affect traffic, but eventually to clear this alarm, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.147 LASERBIAS-FAIL

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Bias Failure (LASERBIAS-FAIL) alarm occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when a failure occurs on the card laser current control circuit, or if the laser is broken.

Clear the LASERBIAS-FAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 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. Refer to 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, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.148 LASEREOL

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Laser Approaching End of Life (LASEREOL) alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It is typically accompanied by the "HI-LASERBIAS" alarm on page 2-101. It is an indicator that the laser in the card will need to be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, the card must be replaced sooner.

Clear the LASEREOL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.149 LASERTEMP-DEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Temperature Degrade (LASERTEM-DEG) condition occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when a failure occurs on the laser Peltier control circuit that degrades laser performance in the amplifier card.

Clear the LASERTEMP-DEG Alarm

Step 1 This alarm does not immediately affect traffic, but eventually to clear this alarm, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *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 condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.150 LKOUTPR-S

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Lockout of Protection Span (LKOUTPR-S) condition occurs on a BSLR node when traffic is locked out of a protect span using the Lockout Protect Span command.

Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.151 LKOUTWK-S (NA)

The LKOUTWK-S condition is not supported in this release. It is reserved for future development.

2.7.152 LMP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UCP-IPCC

The Link Management Protocol (LMP) Hello Down alarm (LMP-HELLODOWN) occurs when the Hello protocol, which monitors UCP control channel status, is not available for link management. The unavailability can be caused by physical layer errors (such as cabling) or by control channel misconfiguration.

Clear the LMP-HELLODOWN Alarm

Step 1 Verify that transmit and receive cables are not crossed at each end (login site and neighbor site).

Step 2 Verify that the "LOF (OCN)" alarm on page 2-123 is not present on the source or destination nodes. If so, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 3 If the alarm does not clear, complete the "Clear the CKTDOWN Alarm" procedure on page 2-51 to verify that IPCC provisioning is valid on both ends of the UNI.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.153 LMP-NDFAIL

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

- Logical Object: UPC-IPCC

The LMP Neighbor Detection Fail (LMP-NDFAIL) alarm occurs when neighbor detection within the UCP has failed. LMP-NDFAIL can be caused by physical failure (such as cabling) between the neighbors or by control channel misconfiguration.

Clear the LMP-NDFAIL Alarm

Step 1 Complete the "Clear the LMP-HELLODOWN Alarm" procedure on page 2-118.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.154 LOA

- Critical (CR), Service-Affecting (SA)
- Logical Object: VCG

The Loss of Alignment (LOA) on a virtual concatenation group (VCG) is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.

Note This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

Step 1 In network view, click the Circuits tab.

Step 2 Click the alarmed VCG and then click Edit.

Step 3 In the Edit Circuit dialog box, click **Show Detailed Map** to see the source and destination circuit slots, ports, and STSs.

Step 4 Identify whether the STS travels across different fibers. If it does, complete the "Delete a Circuit" procedure on page 2-217.

Step 5 Recreate the circuit using the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.155 LOCKOUT-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Lockout Switch Request on Facility or Equipment (LOCKOUT-REQ) condition occurs when a user initiates a lockout switch request for an OC-N card or a lockout switch request on a path protection at the path level. A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear a Path Protection Lockout" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.156 LOF (BITS)

- Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC2 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.

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.

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

Clear the LOF (BITS) Alarm

Step 1 Verify that the line framing and line coding match between the BITS input and the TCC2:

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

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

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

d. Verify that Coding matches the coding of the BITS timing source, either B8ZS or AMI.

e. If the coding does not match, click **Coding** and choose the appropriate coding from the pull-down menu.

f. Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

g. If the framing does not match, click **Framing** and choose the appropriate framing from the pull-down menu.

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

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2, complete the "Physically Replace a Card" procedure on page 2-219 for the TCC2 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.157 LOF (CLIENT)

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Loss of Frame for a DWDM client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It is raised when the card port has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (CLIENT) Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-124.

Step 2 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.158 LOF (DS1)

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream. If the LOF appears on the DS1-N-14 card, the transmitting equipment could have its framing set to a format that differs from the receiving ONS 15454.

Clear the LOF (DS1) Alarm

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

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

b. Find the coding and framing formats of the signal source for the card reporting the alarm. You may need to contact your network administrator for the format information.

c. Display the card view of the reporting card.

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

e. Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a pull-down menu and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source's line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the Line Coding cell and choose the right type from the pull-down menu.

g. Click **Apply**.

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

Note When you replace a card with 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.159 LOF (DS3)

- Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment could be set to a format that differs from the receiving ONS 15454. On DS3XM-6 cards, the alarm occurs only on cards with the provisionable framing format set to C bit or M13 and not on cards with the provisionable framing format is set to unframed.

Clear the LOF (DS3) Alarm

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

a. Display the card view of the reporting card.

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

c. Verify that the line type of the reporting port matches the line type of the signal source.

d. If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the pull-down menu.

e. Click **Apply**.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.160 LOF (EC1-12)

- Critical (CR), Service-Affecting (SA)
- Logical Object: EC1-12

The EC1-12 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.

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 LOF (EC1-12) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure 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 conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.161 LOF (OCN)

- Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The LOF alarm occurs when a port on the reporting OC-N, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G 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 at the lower-right outside edge of the shelf assembly.

Clear the LOF (OCN) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure 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 conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.162 LOF (TRUNK)

- Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Frame for the DWDM trunk applies to the trunk optical or electrical signal that is carried to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It indicates that the receiving ONS 15454 has lost frame delineation in the incoming data from trunk that serves the cards. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (TRUNK) Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-124.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.163 LOM

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSTRM, TRUNK, VT-TERM

The optical transport unit (OTU) Loss of Multiframe (LOM) is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than three milliseconds.

Clear the LOM Alarm

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.164 LOP-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Loss of Pointer Path (LOP-P) alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

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 LOP-P Alarm

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS 3c instead of an STS1, this will cause the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.

Step 4 If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-217.

Step 5 Recreate the circuit for the correct size. For instructions, see the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.165 LOP-V

- Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

The LOP VT (LOP-V) alarm indicates a loss of pointer at the VT level.

The LOP-V alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

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 LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-125.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.166 LO-RXPOWER

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN

The Equipment Low Receive Power (LO-RXPOWER) alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.

Note If the card is part of an amplified dense wavelength division multiplexing system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

Step 4 If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

Step 5 If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error readings you get will not be as precise, but you will generally know whether the fiber is faulty.

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

Step 7 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the "Perform a Facility (Line) Loopback on a Source DS-N Port (West to East)" procedure on page 1-8.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Card" procedure on page 2-219. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 no ports are shown bad and the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.167 LOS (BITS)

- Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2 card has an LOS from the BITS timing source. The 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 at the lower-right outside edge of the shelf assembly.

Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.168 LOS (CLIENT)

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Loss of Signal for a DWDM client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Note The alarm severity of the client-side Loss of Signal (LOS) alarm is based on the protection status of the card; a critical (CR) alarm is raised for a working card and a minor (MN) alarm is raised for a standby card. If a working card has an active LOS alarm, the alarm severity is CR even though the circuit is protected.

Clear the LOS (CLIENT) Alarm

Step 1 Complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.169 LOS (DS1)

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A LOS (DS-1) alarm for a DS-1 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.

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 LOS (DS1) Alarm

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

If an optical TDM signal such as an OC-3 or OC-12 is plugged into an E1000-2 or G1000-4 card GBIC connector, this can trigger an LOS.

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is not currently assigned, place the port out of service using the following steps. LOS can be caused by a non-assigned port placed in service (IS).

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

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

c. Look under the State column to determine the port's status.

Step 4 If the port is assigned, verify that the correct port is in service:

a. To confirm this physically, confirm that the card shows a green LED on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine this virtually, 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 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 7 If there is a valid signal, replace the electrical connector on the ONS 15454.

Step 8 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port.

Step 9 Repeat Steps 1 to 8 for any other port on the card that reports the LOS.

Step 10 If no other alarms are present that could be the source of the LOS (DS-1), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 11 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.170 LOS (DS3)

- Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The LOS (DS-3) for a DS-3 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 at the lower-right outside edge of the shelf assembly.

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (DS3) Alarm

Step 1 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-128.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.171 LOS (EC1-12)

- Critical (CR), Service-Affecting (SA)
- Logical Object: EC1-12

LOS on an EC1-12 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC1-12) means that the upstream transmitter has failed. If an EC1-12 LOS alarm is not accompanied by additional alarms, a 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 at the lower-right outside edge of the shelf assembly

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (EC1-12) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

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

c. 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 cable connector on the ONS 15454.

Step 6 Repeat Steps 1 through 5 for any other port on the card that reports the LOS (EC1-12).

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 8 If no other alarms exist that could be the source of the LOS (EC1-12), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.172 LOS (FUDC)

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: FUDC

The LOS on the F1 user data channel (FUDC) alarm is raised if there is a UDC circuit created on the AIC-I DCC port but the port is not receiving signal input. The downstream node will have an AIS condition raised against the AIC-I DCC port transmitting the UDC.

Clear the LOS (FUDC) Alarm

Step 1 Verify cable continuity to the AIC-I UDC port.

Step 2 Verify that there is a valid input signal using a test set.

Step 3 If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 4 If the alarm does not clear, verify that the UDC is provisioned:

a. At the network view, click the **Provisioning > Overhead Circuits** tabs.

b. If no UDC circuit exists, create one. Refer to the *Cisco ONS 15454 Procedure Guide*.

c. If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.

Step 5 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 6 If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 7 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.173 LOS (MSUDC)

The LOS alarm for the MSUDC is not supported in this platform in this release. It is reserved for future development.

2.7.174 LOS (OCN)

- Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

A LOS alarm on an OC-N port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS alarm means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. 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 could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (OCN) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber 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 according to site practice. If no site practice exists, complete the procedure 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 "OC-N Card Transmit and Receive Levels" section on page 1-102 lists these specifications for each OC-N card, and the *Cisco ONS 15454 Reference Manual* lists levels for DWDM cards.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 7 Repeat Steps 1 to 6 for any other port on the card reporting the LOS (OC-N).

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS (OC-N), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.175 LOS (OTS)

- Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The Loss of Signal for the optical transport section (OTS) applies to add/drop, amplifier, multiplexer, demultiplexer, and combiner cards. It indicates that there is a loss or received signal at the OSCM, OSC-CSM card or OPT-BST card port. Troubleshooting for this alarm is similar to LOS (OCN), page 2-132.

Clear the LOS (OTS) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin value of the Line 4-1-RX port) is within the expected range shown in Cisco MetroPlanner. To check the level:

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

b. Click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.

c. Compare the opwrMin (dBm) column value with the MetroPlanner-generated value. (For more information about using MetroPlanner, refer to the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5*.

Step 4 If the optical power level is within specifications, check and modify the channel LOS and OSC LOS thresholds, then run automatic node setup (ANS) to execute the changes:

a. In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

b. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to decide what values to use, then modify the following items:

- West Side Rx. Channel OSC LOS Threshold
- West Side Rx. Channel LOS Threshold

c. Click the **WDM-ANS > Port Status** tabs.

d. Click **Launch ANS** and click **Yes** in the confirmation dialog box.

Step 5 If the optical power is outside of the expected range, check the power level transmitted at the other side of the span using CTC:

a. On the transmitting node, double-click the transmitting MXP or TXP to display the card view.

b. Click the **Provisioning > Optics Thresholds** tab.

c. View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.

Step 6 If the transmitted power value is within the expected range, clean the receiving node (where the LOS is raised) and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 7 If the transmitted power value is outside of the expected range, troubleshoot using the DWDM acceptance tests in the *Cisco ONS 15454 Procedure Guide*.

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

⚠ **Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Alarm Procedures" section on page 2-21 for commonly used lockout and traffic-switching procedures. For detailed information and guidelines for traffic switching, refer to the *Cisco ONS 15454 Procedure Guide*.

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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.176 LOS (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Signal for a TRUNK applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Clear the LOS (TRUNK) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as **IS**.

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *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 TXP or MXP card receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for levels.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 7 Repeat Steps 1 to 6 for any other port on the card reporting the LOS (TRUNK).

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Verify or Create Node DCC Terminations" section on page 2-214 for commonly used procedures.

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 into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.177 LOS-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: CLIENT, TRUNK

The Path Loss of Signal (LOS-P) alarm applies to all input ports of AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-BST, 32MUX-O, 32DMX-O, and OSC-CSM cards when there is a loss of received signal at an input port caused by MXP or TXP transmit port errors.

Clear the LOS-P Alarm

Step 1 Check the fiber cable connection between the MXP or TXP card and the DWDM card.

Step 2 Verify that the MXP or TXP card TRUNK TX port is in IS state. If not, change the state to IS:

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

b. For the port, choose IS from the State column.

Step 3 If port state is IS, check the output power on the transmit MXP or TXP card using CTC:

- **a.** On the transmitting node, double-click the card to display the card view.
- **b.** Click the **Performance > Optics PM** tab.
- **c.** Under the **Param** column, view the TX Optical Pwr value for the port.

Step 4 Check this value against the TXP or MXP specifications.

Step 5 If the value is within specifications, proceed to Step 6. If the value is outside of specifications, complete the following steps to turn on the OCHN connection and clear the LOS-P alarm:

- **a.** If you are not already in card view for the alarmed card, double-click it to display the card view.
- **b.** Click the **Provisioning> Optical Thresholds** tab.
- **c.** Identify the provisioned **VOA Attenuation Reference** parameter.
- **d.** Double-click **VOA Attenuation Calibration** and enter a value exactly opposite to the VOA attenuation reference value. For example, if the reference value is 20 dBm, set the calibration value at –20 dBm.
- **e.** Click **Apply**.

Note This procedure only temporarily adjusts system optical performance. An out-of-specification TXP or MXP card must eventually be replaced to guarantee system optical performance.

Step 6 If the alarm does not clear, look for any other upstream alarm that could be identified as the source of the problem.

Step 7 If no other alarms that could be the source of the LOS-P exist, place all of the card ports in OOS state.

Step 8 Complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS state.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.178 LO-TXPOWER

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Equipment Low Transmit Power (LO-TXPOWER) alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-TXPOWER Alarm

Step 1 Display the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card view.

Step 2 Click the **Provisioning > Optical Thresholds** tabs.

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 no ports are shown bad and the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.179 LPBKCRS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Loopback Cross-Connect (LPBKCRS) condition indicates that there is a software cross-connect loopback active between a traffic (optical) card and an XC10G cross-connect card. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Note XC loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the traffic (optical) card in CTC to display the card view.

Step 2 Click the **Provisioning > SONET STS** tabs.

Step 3 In the **XC Loopback** column, deselect the check box for the port.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.180 LPBKDS1FEAC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Caused by Far-End Alarm and Control (FEAC) Command DS-1 condition (LPBKDS1FEAC) on the DS3XM-6 card occurs when a DS-1 loopback signal is received from the far-end node due to a FEAC command. An FEAC command is often used with loopbacks.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKDS1FEAC Condition

Step 1 In node view, double-click the DS3XM-6 card to display the card view.

Step 2 Click the **Maintenance > DS1** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the pull-down menu.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.181 LPBKDS1FEAC-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The LPBKDS1FEAC Command Sent (LPBKDS1FEAC-CMD) condition occurs on the near-end node when you send a DS-1 FEAC loopback. For more information about FEAC loopbacks, see the "Using the DS3XM-6 Card FEAC (Loopback) Functions" section on page 1-35.

Note LPBKDS1FEAC-CMD is an informational condition. It does not require troubleshooting.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

2.7.182 LPBKDS3FEAC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

A Loopback Due to FEAC Command DS-3 (LPBKDS3FEAC) condition occurs when a DS3XM-6 or DS3-12E card loopback signal is received from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by DS3XM-6 cards and DS3-12E cards. A DS3XM-6 card both generates and reports FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

Note LPBKDS3FEAC is an informational condition. It does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

Step 1 In node view, double-click the DS-3 card to display the card view.

Step 2 Click the **Maintenance > DS3** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the pull-down menu.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.183 LPBKDS3FEAC-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The LPBKDS3FEAC Command Sent (LPBKDS3FEAC-CMD) condition occurs on the near-end node when you send a DS-3 FEAC loopback. For more information about FEAC loopbacks, see the "Using the DS3XM-6 Card FEAC (Loopback) Functions" section on page 1-35.

Note LPBKDS3FEAC-CMD is an informational condition. It does not require troubleshooting.

2.7.184 LPBKFACILITY (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

A Loopback Facility (LPBKFACILITY) condition on TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards occurs when a port has a software facility (line) loopback active.

For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (CLIENT, TRUNK) Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.185 LPBKFACILITY (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting DS-1 or DS-3.

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 1-8.

Note CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

Note DS-3 facility (line) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Clear the LPBKFACILITY (DS1, DS3) Condition

Step 1 In node view, double-click the reporting DS3XM-6 card to display the card view.

Step 2 Click the **Maintenance > DS3** tab.

If the condition is reported against a DS-1 line, also click the **DS1** tab.

Step 3 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.186 LPBKFACILITY (EC1-12)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EC1-12

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting EC1-12 card.

For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (EC1-12) Condition

Step 1 The loopback originates from the DS3XM-6 card. Complete the "Clear the LPBKDS3FEAC Condition" procedure on page 2-140.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.187 LPBKFACILITY (G1000)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting G1000 Ethernet card.

For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (G1000) Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.188 LPBKFACILITY (OCN)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting OC-N card.

For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Note OC-3 facility loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (OCN) Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

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

2.7.189 LPBKTERMINAL (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

A Loopback Terminal (LPBKTERMINAL) condition occurs when a software terminal (inward) loopback is active for a TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card port.

For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-8.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (CLIENT) Condition

Step 1 Complete the "Clear the LPBKFACILITY (CLIENT, TRUNK) Condition" procedure on page 2-141.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.190 LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3, EC1-12, OCN

A LPBKTERMINA) condition occurs when a software terminal (inward) loopback is active for a port on the reporting card. DS-N and OC-N terminal loopbacks do not typically return an AIS.

Note DS-3 and EC-1 terminal (inward) loopbacks do not transmit an in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Note Performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

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

Clear the LPBKTERMINAL (DS1, DS3, EC1-12, OCN) Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note Terminal (inward) loopback is not supported at the DS-1 level for the DS3XM-6 card.

2.7.191 LPBKTERMINAL (G1000)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A LPBKTERMINAL condition occurs when a software terminal (inward) loopback is active for a port on the reporting G-1000 Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-4 card the outgoing signal is not transmitted; it is only redirected in the receive direction.

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

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (G1000) Condition

Step 1 Complete the "Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback" procedure on page 2-217.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.192 LWBATVG

- Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Low Voltage Battery (LWBATVG) alarm occurs in a –48 VDC environment when a battery lead's input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide*.)

Clear the LWBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.193 MAN-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Manual Switch Request (MAN-REQ) condition occurs when a user initiates a Manual switch request on an OC-N card or path protection path. Clearing the Manual switch clears the MAN-REQ condition.

Clear the MAN-REQ Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.194 MANRESET

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

A User-Initiated Manual Reset (MAN-RESET) condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

Note MANRESET is an informational condition. It does not require troubleshooting.

2.7.195 MANSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Manual Switch To Internal Clock (MANSWTOINT) condition occurs when the NE timing source is manually switched to the internal timing source.

Note MANSWTOINT is an informational condition. It does not require troubleshooting.

2.7.196 MANSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference (MANSWTOPRI) condition occurs when the NE timing source is manually switched to the primary timing source.

Note MANSWTOPRI is an informational condition. It does not require troubleshooting.

2.7.197 MANSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference (MANSWTOSEC) condition occurs when the NE timing source is manually switched to the second timing source.

Note MANSWTOSEC is an informational condition. It does not require troubleshooting.

2.7.198 MANSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference (MANSWTOTHIRD) condition occurs when the NE timing source is manually switched to the tertiary timing source.

Note MANSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.7.199 MANUAL-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Manual Switch Request on Ring (MANUAL-REQ-RING) condition occurs when a user initiates a MANUAL RING command on two-fiber and four-fiber BLSR rings to switch from working to protect or protect to working.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.200 MANUAL-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Manual Switch Request on Span (MANUAL-REQ-SPAN) condition occurs on four-fiber BLSRs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span.

Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-215.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.201 MEA (AIP)

- Critical (CR), Service-Affecting (SA)
- Logical Object: AIP

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-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

Clear the MEA (AIP) Alarm

Step 1 Complete the "Replace the Alarm Interface Panel" procedure on page 3-12.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.202 MEA (EQPT)

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet (traffic) cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly. Removing the incompatible cards clears the alarm.

Note If an OC3-8 card is installed in Slots 5 to 6 and 12 to 13, it does not appear in CTC and raises an MEA.

Note When a failed member of an XC pair is field-replaced with an XCVT card, the "CTNEQPT-MISMATCH" alarm on page 2-58 is raised rather than the MEA alarm.

Clear the MEA (EQPT) Alarm

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

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf

Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.

Note On the 15454-SA-HD (P/N: 800-24848),15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

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

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

b. If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet (traffic) 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, noncompatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a 10-Gbps-compatible shelf assembly.

c. If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the XC10G, OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to Step 3.

d. If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the 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 In 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" procedure on page 2-219 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 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, 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, CTC does not allow you to delete the card.

Step 6 If any ports on the card are in service, place them out of service (OOS):

⚠ **Caution** Before placing ports out of service, ensure that live traffic is not present.

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" procedure on page 2-217.

⚠ **Caution** Before deleting the circuit, ensure that live traffic is not present.

Step 8 If the card is paired in a protection scheme, delete the protection group:

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

b. Choose the protection group of the reporting card.

c. Click **Delete**.

Step 9 Right-click the card reporting the alarm.

Step 10 Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Step 11 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.203 MEA (FAN)

- Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

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

Clear the MEA (FAN) Alarm

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

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD.

Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.

Step 2 If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5 A fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 3-10.

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 3-10.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.204 MEM-GONE

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Memory Gone (MEM-GONE) alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2 card. CTC does not function properly until the alarm clears. The alarm clears when additional memory becomes available.

Note The alarm does not require user intervention. If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.205 MEM-LOW

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Free Memory of Card Almost Gone (MEM-LOW) alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2 card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC2 card is exceeded, CTC ceases to function.

Note The alarm does not require user intervention. If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.206 MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN)

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, BPLANE, FAN

The Manufacturing Data Memory Failure (MFGMEM) alarm occurs if the ONS 15454 cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC2 lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EEPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address disrupts IP connectivity and grays out the ONS 15454 icon on the CTC network view.

Clear the MFGMEM (AICI-AEP, AIE, BPLANE, FAN) Alarm

Step 1 Complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 2 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

Step 3 If the MFGMEM alarm continues to report after replacing the TCC2 cards, the problem is with the EEPROM.

Step 4 If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 3-10.

Step 5 If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.207 NO-CONFIG

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The No Startup Configuration (NO-CONFIG) condition applies to ML-Series Ethernet (traffic) cards and occurs when you preprovision Slots 5 to 6 and 12 to 13 for the card without inserting the card first, or when you insert a card without preprovisioning. (This is an exception to the usual rule in card provisioning.) Because this is normal operation, you should expect this alarm during provisioning. When the startup configuration file is copied to the active TCC2, the alarm clears.

Clear the NO-CONFIG Condition

Step 1 Create a startup configuration for the card in IOS.

Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

Step 2 Upload the configuration file to the TCC2:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.208 NOT-AUTHENTICATED

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

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm on page 2-111 in that INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.7.209 NTWTPINC

The NTWTPINC condition is not used in this platform in this release. It is reserved for future development.

2.7.210 OCHNC-ACTIV-FAIL

The OCHNC-ACTIV-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.211 OCHNC-DEACTIV-FAIL

The OCHNC-DEACTIV-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.212 OCHNC-FAIL

The OCHNC-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.213 OCHNC-INC

The OCHNC-INC alarm is not used in this platform in this release. It is reserved for future development.

2.7.214 ODUK-AIS-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition (ODUK-AIS-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the "LOS (OCN)" alarm on page 2-132 occurring downstream. The ODUK-AIS-PM condition is reported in the path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by the upstream "ODUK-OCI-PM" condition on page 2-155.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-AIS-PM Condition

Step 1 Determine whether upstream nodes and equipment have alarms, especially the "LOS (OCN)" alarm on page 2-132, or OOS ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.215 ODUK-BDI-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition (ODUK-BDI-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead. ODUK-BDI-PM occurs when the "PORT-CODE-MISM" condition on page 2-168 occurs upstream.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP cards or MXP cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-BDI-PM Condition

Step 1 Complete the "Clear the OTUK-BDI Condition" procedure on page 2-162.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.216 ODUK-LCK-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition (ODUK-LCK-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-LCK-PM Condition

Step 1 Unlock the upstream node signal.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.217 ODUK-OCI-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition (ODUK-OCI-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes an "ODUK-LCK-PM" condition on page 2-155 downstream.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-OCI-PM Condition

Step 1 Verify the fiber connectivity at nodes upstream.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.218 ODUK-SD-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line bit error rate (BER) has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-SD-PM Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.219 ODUK-SF-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-SF-PM Condition

Step 1 Complete the "Clear the SF (DS1, DS3) Condition" procedure on page 2-182.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.220 ODUK-TIM-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The ODUK Trace Identifier Mismatch (TIM) PM condition (ODUK-TIM-PM) applies to the path monitoring area of the OTN overhead for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes a "ODUK-BDI-PM" condition on page 2-154 downstream.

The ODUK-TIM-PM condition applies to TX cards and MXP cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-TIM-PM Condition

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-199.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.221 OOU-TPT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure (OOU-TPT) alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused. It occurs in conjunction with the "VCG-DEG" alarm on page 2-206.

Clear the OOT-TPT Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-207. Clearing that condition clears this condition as well.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.222 OPTNTWMIS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Optical Network Type Mismatch (OPNTWMIS) alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore and MetroAccess. All DWDM nodes on the same network must be configured for the same network type because automatic power control (APC) and automatic node setup (ANS) behave differently on each of these network types.

When the OPTNTWMIS occurs, the "APC-DISABLED" alarm on page 2-24 could also be raised.

Clear the OPTNTWMIS Alarm

Step 1 In node view of the alarmed node, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Choose the correct option from the Network Type list box, and click **Apply**.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.223 OPWR-HDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power High Degrade alarm occurs on all DWDM ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, and 32MUX-O card OCH ports, and the OSC-CSM and OSCM OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the high degrade threshold. For 32DMX, 32DMX-O, and 32MUX-O OCH ports and OSC-CSM and OSCM OSC-TX ports, OPWR-HDEG indicates that the card has a variable optical attenuator (VOA) control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-HDEG Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the power read by photodiode on the port is within the expected range foreseen by MetroPlanner. The application generates a spreadsheet of values containing this information.

Step 4 If the optical power level is within specifications, check the opwrMin threshold. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* and decide what value to use for modifying the value:

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

b. Display the optical thresholds by clicking the following tabs:

- OPT-BST **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- OPT-PRE **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- AD-xC **Provisioning > Optical Chn> Optics Thresholds** tab

- AD-xB **Provisioning > Optical Band > Optics Thresholds** tab
- 32DMX **Provisioning > Optical Chn > Optics Thresholds** tab
- 32MUX **Provisioning > Optical Chn > Optics Thresholds** tab
- OSCM **Provisioning > Optical Line > Optics Thresholds** tab

Step 5 If the received optical power level is within specifications, consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to determine the correct levels and check the opwrMin threshold. If necessary, modify the value as required.

Step 6 If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS admin state by clicking the correct tab:

- MXPP_MR_2.5G **Provisioning > Line > OC48** tab
- MXP_2.5G_10E **Provisioning > Line > Trunk** tab
- MXP_2.5G_10G **Provisioning > Line > SONET** tab
- MXP_MR_2.5G **Provisioning > Line > OC48** tab
- TXPP_MR_2.5G **Provisioning > Line > OC48** tab
- TXP_MR_10E **Provisioning > Line > SONET** tab
- TXP_MR_10G **Provisioning > Line > SONET** tab
- TXP_MR_2.5G **Provisioning > Line > SONET** tab

If it is not IS, choose **IS** from the state drop-down list.

Step 7 If the port is in IS state but its output power is outside of the specifications, complete the "Clear the LOS-P Alarm" procedure on page 2-136.

Step 8 If the signal source is IS and within expected range, come back to the unit reporting OPWR-HDEG and clean all connected fiber in the same line direction as the reported alarm according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the "Alarm Procedures" section on page 2-21. For more detailed protection switching information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 9 Repeat Steps 1 to 8 for any other port on the card reporting the OPWR-HDEG alarm.

Step 10 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 11 If no other alarms exist that could be the source of the OPWR-HDEG, or if clearing an alarm did not clear the alarm, place all of the card ports in OOS,DSBLD admin state.

Step 12 Complete the "Physically Replace a Card" procedure on page 2-219 for the reporting card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS state.

Step 13 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.224 OPWR-HFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Optical Power Fail High (OPWR-FAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE amplifier cards on the Line-1 TX port when an internal card problem on the card prevents the card from maintaining the output power setpoint at the output port and the card fails. It occurs on optical add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x); demultiplexers (32 DMX-O); combiners (4MD-xx.x), and optical service channel cards (OSCM and OSC-CSM) when there is a failure on the VOA circuit.

Clear the OPWR-HFAIL Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-158. (This procedure clears all optical power level degrade and fail alarms.)

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.225 OPWR-LDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Low Degrade alarm occurs on all ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, and 32MUX-O card OCH ports; and the OSC-CSM and OSCM card OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the low degrade threshold. For the 32DMX, 32DMX-O, and 32MUX-O card OCH ports and the OSC-CSM and OSCM card OSC-TX ports, OPWR-HDEG indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-LDEG Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-158. (This procedure clears all optical power level degrade and fail alarms.)

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.226 OPWR-LFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm applies to OPT-BS T and OPT-PRE amplifier AOTS ports. It also applies to AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32DMX, and OSC-CSM transmit (TX) ports. The alarm is raised when monitored input power crosses the low fail threshold.

For the AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x card OCH ports and the 32MUX-O, 32DMX, 32DMX-O, OSCM, and OSC-CSM cards, OPWR-LFAIL indicates that the card has a VOA control circuit failure that affects its attenuation capability.

Clear the OPWR-LFAIL Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-158. (This procedure clears all optical power degrade and fail alarms.)

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.227 OTUK-AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition (OTUK-AIS) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition, such as the "LOS (OCN)" alarm on page 2-132, is occurring downstream. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.228 OTUK-BDI

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-BDI condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-BDI is indicated by the BDI bit in the section monitoring overhead. The alarm occurs when there is an SF condition upstream. OTUK-BDI is triggered by the "OTUK-TIM" condition on page 2-164.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-BDI Condition

Step 1 Determine whether upstream nodes have the "OTUK-AIS" condition on page 2-161.

Step 2 In the upstream node, click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card in node view to display the card view.

Step 3 Click the **Provisioning > OTN > Trail Trace Identifier** tabs.

Step 4 Compare the Current Transmit String with the Current Expected String in the downstream node. (Verify the Current Expected String by making the same navigations in another CTC session to the downstream node.)

Step 5 If the two do not match, modify the Current Expected String.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.229 OTUK-LOF

- Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The OTUK-LOF alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card of MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-LOF Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-124.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.230 OTUK-SD

- Not Alarmed (NA) Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SD condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-SD Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.231 OTUK-SF

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SF condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-SF Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.232 OTUK-TIM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-TIM alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled and section trace mode is set to manual. The alarm indicates that the expected TT1 string does not match the received TTI string in the optical transport unit overhead of the digital wrapper. OTUK-TIM triggers an "ODUK-BDI-PM" condition on page 2-154.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-TIM Condition

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-199.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.233 OUT-OF-SYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The Ethernet Out of Synchronization (OUT-OF-SYNC) condition occurs on TXP-MR-2.5 and TXPP-MR-2.5 cards when the card ports are not correctly configured for the Ethernet payload data type.

Clear the OUT-OF-SYNC Condition

Step 1 Double-click the alarmed card to display the card view.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 In the **Payload Data Type** drop-down list, choose **Ethernet**.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.234 PDI-P

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The PDI Path condition (PDI-P) is a set of application-specific codes contained in the STS path overhead (POH) generated by the ONS node. The alarm indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE), for example, to the path selector in a downstream ONS node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

The "AIS" condition on page 2-21 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 could result from the end-to-end Ethernet link integrity feature of the G1000-4. If the link integrity is the cause, it is typically accompanied by the "TPTFAIL (G1000)" alarm on page 2-200 or the "CARLOSS (G1000)" alarm on page 2-46 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.

A PDI-P condition reported on the port of an OC-N card supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the "TPTFAIL (G1000)" alarm on page 2-200 alarm reported against one or both packet over SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of packet over SONET (POS) ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for more information about ML-Series cards.

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

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Clear the PDI-P Condition

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

a. Click the **Circuits** tab.

b. Verify that the Status column lists the port as active.

c. If the Status column lists the port as incomplete, wait 10 minutes for the ONS 15454 to initialize fully. If the incomplete state does not change after full initialization, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC 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" procedure on page 2-217.

Caution Deleting a circuit could affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 5 If circuit deletion and recreation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 8 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-219 for the optical/electrical (traffic) 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.235 PEER-NORESPONSE

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Peer Card Not Responding (PEER-NORESPONSE) alarm is raised by the switch agent if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.236 PLM-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path (PLM-P) alarm indicates that signal does not match its label. The condition occurs due to an invalid C2 byte value in the SONET path overhead.

For example, on non-DWDM nodes, this condition can occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

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

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Clear the PLM-P Alarm

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-165.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.237 PLM-V

- Major (MJ), Service-Affecting (SA)
- Logical Object: VT-TERM

A PLM VT Layer (PLM-V) 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.

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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.238 PORT-CODE-MISM

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Pluggable Port Security Code Mismatch (PORT-CODE-MISM) alarm refers to ML-Series Ethernet (traffic) cards, MXP_2.5G_10Gs, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5Gs. PORT-CODE-MISM occurs when the SFP connector that is plugged into the card is not supported by Cisco.

Clear the PORT-CODE-MISM Alarm

Step 1 Unplug the SFP connector and fiber from the reporting card.

Step 2 If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

Step 3 Pull the fiber cable straight out of the connector.

Step 4 Plug the fiber into a Cisco-supported SFP connector.

Step 5 If the new SFP connector has a latch, close the latch over the cable to secure it.

Step 6 Plug the cabled SFP connector into the card port until it clicks.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.239 PORT-COMM-FAIL

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Port Communication Failure (PORT-COMM-FAIL) alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card SFPs. It occurs when the card cannot communicate with the SFP.

Clear the PORT-COMM-FAIL Alarm

Step 1 Replace the faulty SFP with a new SFP:

a. Unplug the SFP connector and fiber from the ML-Series Ethernet (traffic) card.

b. If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

c. Pull the fiber cable straight out of the connector.

d. Plug the fiber into a Cisco-supported SFP connector.

e. If the new SFP connector has a latch, close the latch over the cable to secure it.

f. Plug the cabled SFP connector into the ML-Series Ethernet card port until it clicks.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.240 PORT-MISMATCH

- Critical (CR), Service-Affecting (CLIENT)
- Not Alarmed (NA), Non-Service Affecting (NSA) for FCMR
- Logical Objects: CLIENT, FCMR

The Pluggable Port Mismatch (PORT-MISMATCH) alarm applies to ML-Series Ethernet (traffic) card and TXP card SFP connectors. The alarm indicates that the provisioned payload for the connector does not match the SFP configuration.

The error must be resolved in the IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*. If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.241 PORT-MISSING

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Pluggable Port Code Missing (PORT-MISSING) alarm applies to ML-Series Ethernet (traffic) card SFP connectors. The alarm indicates that the connector is not plugged into the card port.

For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

Clear the PORT-MISSING Alarm

Step 1 If fiber is not plugged into the SFP connector, plug it in.

Step 2 If the SFP connector has a latch, pull the latch over the connector.

Step 3 Push the SFP connector into the ML-Series Ethernet (traffic) card port until it clicks in place.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.242 PRC-DUPID

- Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The Procedural Error Duplicate Node ID (PRC-DUPID) alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213.

Step 3 Repeat Step 2 for all the nodes on the ring.

Step 4 If two nodes have an identical node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-214 so that each node ID is unique.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.243 PROTNA

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Protection Unit Not Available (PROTNA) alarm is caused by an OOS protection card when a TCC2 or XC10G cross-connect card that is provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if it is raised against a common control card (TCC2 or cross-connect), 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, verify that the ports have been taken out of service (OOS):

a. In CTC, double-click the reporting card to display the card view (if the card is not an XC10G cross-connect card).

b. Click the **Provisioning** tab.

c. Click the **State** of any in-service (IS) ports.

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

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the reporting card.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.244 PTIM

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Payload Type Identifier Mismatch (PTIM) alarm occurs when there is a mismatch between the way the ITU-T G.709 option is configured on MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card at each end of the optical span.

Clear the PTIM Alarm

Step 1 Double-click the alarmed MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card to display the card view.

Step 2 Click the **Provisioning > OTN > OTN Lines** tabs.

Step 3 Ensure that the G.709 OTN check box is checked. If not, check it and click Apply.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.245 PWR-A

The PWR-A alarm is not used in this platform in this release. It is reserved for future development.

2.7.246 PWR-B

The PWR-A alarm is not used in this platform in this release. It is reserved for future development.

2.7.247 PWR-REDUN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Redundant Power Capability Lost (PWR-REDUN) alarm applies to cards that have two built-in fuses (such as the TCC2 and newer optical [traffic] cards). The alarm indicates that one of the fuses has blown and must be serviced. When this alarm occurs, the card's power redundancy is lost because only one card power connection can contact one of the redundant power supplies.

Clear the PWR-REDUN Alarm

Step 1 The card fuse is not field-replaceable. Complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 Log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to arrange a card return for service.

2.7.248 RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

The Remote Alarm Indication (RAI) 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 the far-end node is receiving a DS-3 AIS.

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-22.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.249 RCVR-MISS

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Receiver Missing (RCVR-MISS) 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 DS-1 port or a possible mismatch of backplane equipment occurs, for example, an SMB connector or a BNC connector is connected to a DS-1 card.

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

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 RCVR-MISS Alarm

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

Step 2 If the attachment is okay, verify that the cabling is securely connected.

Step 3 If the cabling is okay, 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.250 RFI

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The Remote Failure Indication (RFI) condition is similar to the "RFI-L" condition on page 2-174 but it is raised against an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card when it has the "AIS" condition on page 2-21. The MXP or TXP cards will only raise AIS (or RFI) when they are in line or section termination mode. That is, when the MXP or TXP cards in line termination mode or section termination mode has improperly terminated overhead bytes.

Clear the RFI Condition

Step 1 Complete the "Delete a Circuit" procedure on page 2-217 and then recreate the circuit.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.251 RFI-L

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An RFI Line condition (RFI-L) 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 condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

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

Step 2 Identify and clear any alarms, particularly the "LOS (OCN)" alarm on page 2-132.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.252 RFI-P

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

An RFI Path condition (RFI-P) 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 condition in the reporting node. RFI-P occurs in the node that terminates a path.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS) on the reporting ONS 15454:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green LED indicates an active card. An amber 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 2 To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Clear alarms in the node with the failure, especially the "UNEQ-P" alarm on page 2-204 or the "UNEQ-V" alarm on page 2-206.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.253 RFI-V

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: VT-TERM

An RFI VT Layer (RFI-V) condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

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 RFI-V Condition

Step 1 Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 2 If connectors are correctly connected, verify that the DS-1 port is active and in service (IS):

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green LED indicates an active card. An amber 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, use an optical test set to verify that the signal source does not have errors.

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

Step 4 If the signal is valid, log into the node at the far-end of the reporting ONS 15454.

Step 5 Clear alarms in the far-end node, especially the "UNEQ-P" alarm on page 2-204 or the "UNEQ-V" alarm on page 2-206.

Step 6 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.254 RING-ID-MIS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: OCN, OSC-RING

The Ring ID Mismatch (RING-ID-MIS) condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to BLSR RING-MISMATCH, but rather than apply to ring protection, RING-ID-MIS applies to DWDM node discovery within the same network.

Clear the RING-ID-MIS Alarm

Step 1 Complete the "Clear the RING-MISMATCH Alarm" procedure on page 2-176.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.255 RING-MISMATCH

- Major (MJ), Service-Affecting (SA)
- Logical Objects: OCN, OSC-RING

A Procedural Error Mismatch Ring (RING-MISMATCH) alarm occurs when the ring name of the ONS 15454 that is reporting the alarm does not match the ring name of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical ring names to function. RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.

Clear the RING-MISMATCH Alarm

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 Note the number in the Ring Name field.

Step 3 Log into the next ONS node in the BLSR.

Step 4 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-213.

Step 5 If the ring name matches the ring name in the reporting ONS node, repeat Step 4 for the next ONS node in the BLSR.

Step 6 Complete the "Change a BLSR Ring Name" procedure on page 2-213.

Step 7 Verify that the ring map is correct.

Step 8 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.256 RING-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active East Side (RING-SW-EAST) condition occurs when a ring switch occurs at the east side of two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-EAST is an informational condition. It does not require troubleshooting.

2.7.257 RING-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active West Side (RING-SW-WEST) condition occurs when a ring switch occurs at the west side of a two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-WEST is an informational condition. It does not require troubleshooting.

2.7.258 RSVP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UCP-NBR

The Resource Reservation Protocol (RSVP) Hello Down alarm (RSVP-HELLODOWN) occurs when the Hello protocol, which monitors UCP control channel status, is not available for reserving resources. The lack of availability can be caused by misconfiguration or loss of connectivity between the reporting node and its neighbor.

Clear the RSVP-HELLODOWN Alarm

Step 1 Ensure that there are no physical layer problems between the reporting node and its neighbor.

Step 2 Ensure that neighbor discovery (if enabled) has completed without any errors:

a. In the node CTC view, click the **Provisioning > UCP > Neighbor** tabs.

b. Look for the neighbor ID and address. If it is present, neighbor discovery is working.

Step 3 Ensure that RSVP hello is enabled on the neighbor node. If the neighbor is a Cisco ONS 15454, use the following procedure to ensure that RSVP Hello is enabled on the neighbor. If not, use the corresponding procedure on the core network element:

a. In node view, click **View > Go to Network View**.

b. Double-click the neighbor node in the network map.

c. Click the **Provisioning > UCP > Node** tabs on this neighbor.

d. Ensure that the RSVP area of the window contains entries in the Restart Time, Retransmit Interval, Recovery Time, and Refresh Interval fields.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.259 RUNCFG-SAVENEED

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Run Configuration Save Needed (RUNCFG-SAVENEED) condition occurs when you change the running configuration file for ML1000 and ML100T cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering **copy run start** at the CLI. If you do not save the change, the change is lost after the card reboots.

2.7.260 SD (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

An SD condition occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal degrade threshold. The alarm applies to the card ports (DWDM client) and the trunk carrying optical or electrical signals to the card.

Signal degrade is defined by Telcordia as a soft failure condition. SD and SF both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. The BER threshold on the ONS 15454 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}.

Clear the SD (CLIENT or TRUNK) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.261 SD (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A SD condition for DS-1 or DS-3 occurs when the quality of an electrical signal is so poor that the BER on the incoming optical line has passed the signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and also 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 can be reported on electrical card ports that are in inservice (IS), out-of-service-auto-inservice (OOS-AINS), or auto-inservice (AINS) states, but not in out-of-service (OOS) state. The BER count increase associated with this alarm does not take an IS port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G cross-connect card switches that in turn can cause switching on the lines or paths.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Note Some levels of BER errors (such as 10E_9) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 10E_9 rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SONET ONS electrical cards is the Omniber 718.

Clear the SD (DS1, DS3) Condition

Step 1 Complete the "Verify BER Threshold Level" procedure on page 2-219.

Step 2 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.

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

Step 3 If the optical power level is okay, verify that optical receive levels are within the acceptable range.

Step 4 If receive levels are okay, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 5 If the condition 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 node.

Step 7 If the problem does not clear, the transmitter at the other end of the optical line could 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 8 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.262 SD-L

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SD Line condition (SD-L) is similar to the "SD (DS1, DS3)" condition on page 2-178. It applies to the line level of the SONET signal.

SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The alarm is superseded by higher-priority alarms such as LOF (EC1-12), LOF (OCN), LOS (EC1-12), or LOS (OCN).

Clear the SD-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.263 SD-P

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SD Path condition (SD-P) is similar to the "SD (DS1, DS3)" condition on page 2-178, but it applies to the path (STS) layer of the SONET overhead. A path or ST-level SD alarm travels on the B3 byte of the SONET overhead.

For path 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 path protection, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal degrade and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. SD causes the card to switch from working to protect. The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.264 SF (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

An SF for the DWDM client or trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal fail threshold. The alarm applies to the card ports (DWDM client) and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a soft failure condition. SF monitors the incoming BER and is triggered when the BER surpasses the default range.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Clear the SF (CLIENT, TRUNK) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.265 SF (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

An SF condition for the DS-1 or DS-3 signals 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. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold on the ONS 15454 is user provisionable and has a range for SF from 10^{-5} to 10^{-3}.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Clear the SF (DS1, DS3) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.266 SF-L

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SF Line condition (SF-L) is similar to the "SF (DS1, DS3)" condition on page 2-182, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The alarm is superseded by higher-priority alarms such as LOF (EC1-12), LOF (OCN), LOS (EC1-12), or LOS (OCN).

Clear the SF-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.267 SF-P

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SF Path condition (SF-P) is similar to an "SF-L" condition on page 2-182, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-179.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.268 SFTWDOWN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Software Download in Progress (SFTWDOWN) alarm occurs when the TCC2 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Caution It can take up to 30 minutes for software to be updated on a standby TCC2 card.

Note SFTWDOWN is an informational alarm.

2.7.269 SH-INS-LOSS-VAR-DEG-HIGH

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

The Switch Insertion Loss Variation Degrade High (SH-INS-LOSS-VAR-DEG-HIGH) alarm occurs as the OSC-CSM card optical switch ages and slowly increases its insertion loss. This alarm indicates that the insertion loss has crossed the high degrade threshold. The card will need to be replaced eventually.

2.7.269.1 Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-219 as appropriate.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.270 SH-INS-LOSS-VAR-DEG-LOW

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

The Switch Insertion Loss Variation Degrade Low (SH-INS-LOSS-VAR-DEG-LOW) alarm occurs as the OSC-CSM card optical switch ages and slowly decreases its insertion loss. This alarm indicates that the insertion loss has crossed the low degrade threshold. The card will need to be replaced eventually.

2.7.270.1 Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-219 as appropriate.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

\

2.7.271 SHUTTER-OPEN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The SHUTTER-OPEN alarm occurs if an OSC-CSM card laser shutter remains open after the LOS (OTS) alarm is detected. A laser shutter remains open if an optical safety issue is present and closes when the OSC-CSM card LINE-RX port receives OSC power for three consecutive seconds.

Clear the SHUTTER-OPEN Alarm

Step 1 Complete the "Clear the LOS (OTS) Alarm" procedure on page 2-134.

Step 2 If the SHUTTER-OPEN alarm still does not clear, it indicates that the unit shutter is not working properly. Complete the "Physically Replace a Card" procedure on page 2-219.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.272 SNTP-HOST

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm (SNTP-HOST) indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which could affect the SNTP server/router connecting to the proxy ONS 15454.

Step 3 If no network problems exist, ensure that the ONS 15454 proxy is provisioned correctly:

a. In node view for the ONS node serving as the proxy, click the **Provisioning > General** tabs.

b. Ensure that the Use NTP/SNTP Server check box is checked.

c. If the Use NTP/SNTP Server check box is not checked, click it.

d. Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.

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

2.7.273 SPAN-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active East Side (SPAN-SW-EAST) condition occurs when a span 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 an informational condition. It does not require troubleshooting.

2.7.274 SPAN-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active West Side (SPAN-SW-WEST) condition occurs when a span 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 an informational condition. It does not require troubleshooting.

2.7.275 SQUELCH

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Squelching Traffic (SQUELCH) condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The "AIS-P" condition on page 2-22 also appears on all nodes in the ring except the isolated node.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located at 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 could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.**

Clear the SQUELCH Condition

Step 1 Determine the isolated node:

a. In node view, click **View > Go to Network View**.

b. The grayed out node with red spans is the isolated node.

Step 2 Verify fiber continuity to the ports on the isolated node.

Step 3 If fiber continuity is okay, verify that the proper ports are in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber 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 (traffic) card's receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.

Step 6 If the receiver levels are okay, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are okay, complete the "Physically Replace a Card" procedure on page 2-219 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 8 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.276 SQUELCHED

- Not Alarmed (NA), Non-Service Affecting (SA)
- Logical Object: CLIENT

The CLIENT Signal Squelched (SQUELCHED) alarm is raised by an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card when ITU-T G.709 monitoring is enabled and the card is operating in transparent mode. The alarm occurs on a far-end MXP or TXP card client port when the near end detects the "LOF (OCN)" alarm on page 2-123 or the "LOS (OCN)" alarm on page 2-132. The signal loss is indicated by the "OTUK-AIS" alarm on page 2-161 in the OTN overhead. SQUELCHED can also indicate that the far-end trunk signal is invalid.

Clear the SQUELCHED Alarm

Step 1 Verify that the far-end node and near-end node are not reporting the "LOF (OCN)" alarm on page 2-123 or the "LOS (OCN)" alarm on page 2-132. If so, complete the "Clear the LOF (OCN) Alarm" procedure on page 2-124.

Step 2 If no LOF or LOS is reported, verify that the far-end node and near-end are not reporting the trunk "WVL-MISMATCH" alarm on page 2-210 or the "DSP-FAIL" alarm on page 2-63. If either alarm is reported, complete the "Clear the WVL-MISMATCH alarm" procedure on page 2-210 or the "Clear the DSP-FAIL Alarm" procedure on page 2-64 as appropriate.

Step 3 If no WVL-MISMATCH or DSP-FAIL is reported, verify that the near-end port reporting the SQUELCHED alarm is in service and is not in loopback:

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

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

c. If the port State column says OOS or OOS_MT, click the cell to highlight it and choose **IS** from the pull-down menu. Changing the state to IS also clears any loopback provisioned on the port.

Step 4 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.277 SQM

- Critical (CR), Service-Affecting (SA) for STSTRM
- Major (MJ), Service-Affecting (SA) for VT-TERM
- Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch (SQM) alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

Step 1 For the errored circuit, complete the "Delete a Circuit" procedure on page 2-217.

Step 2 Recreate the circuit using the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.278 SSM-DUS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do-Not-Use (DUS) condition (SSM-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 an informational condition. It does not require troubleshooting.

2.7.279 SSM-FAIL

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The SSM Failed alarm (SSM-FAIL) 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.

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM.

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.280 SSM-LNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The SSM Local Node Clock (LNC) Traceable condition (SSM-LNC) occurs when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.

Note SSM-LNC is an informational condition. It does not require troubleshooting.

2.7.281 SSM-OFF

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The SSM Off condition (SSM-OFF) 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.

Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-189.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.282 SSM-PRC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition (SSM-PRC) occurs when the SONET transmission level is changed to PRC.

Note SSM-PRC is an informational condition. It does not require troubleshooting.

2.7.283 SSM-PRS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Primary Reference Source (PRS) Traceable condition (SSM-PRS) occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note SSM-PRS is an informational condition. It does not require troubleshooting.

2.7.284 SSM-RES

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition (SSM-RES) occurs when the synchronization message quality level is changed to RES.

Note SSM-RES is an informational condition. It does not require troubleshooting.

2.7.285 SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for future development.

2.7.286 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for future development.

2.7.287 SSM-SMC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition (SSM-SMC) occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

Note SSM-SMC is an informational condition. It does not require troubleshooting.

2.7.288 SSM-STU

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Synchronization Traceability Unknown (STU) condition (SSM-STU) occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Clear the SSM-STU Condition

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 If the Sync Messaging **Enabled** check box for the BITS source is checked, uncheck the box.

Step 3 If the Sync Messaging **Enabled** check box for the BITS source is not checked, check the box.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.289 SSM-ST2

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 2 (ST2) Traceable condition (SSM-ST2) occurs when the synchronization message quality level is changed to ST2.

Note SSM-ST2 is an informational condition. It does not require troubleshooting.

2.7.290 SSM-ST3

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 3 (ST3) Traceable condition (SSM-ST3) occurs when the synchronization message quality level is changed to ST3.

Note SSM-ST3 is an informational condition. It does not require troubleshooting.

2.7.291 SSM-ST3E

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 3E (ST3E) Traceable condition (SSM-ST3E) indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is not used for Generation 1.

Note SSM-ST3E is an informational condition. It does not require troubleshooting.

2.7.292 SSM-ST4

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 4 (ST4) Traceable condition (SSM-ST4) occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note SSM-ST4 is an informational condition. It does not require troubleshooting.

2.7.293 SSM-TNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Transit Node Clock (TNC) Traceable condition (SSM-TNC) occurs when the synchronization message quality level is changed to TNC.

Note SSM-TNC is an informational condition. It does not require troubleshooting.

2.7.294 SWMTXMOD

- Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Switching Matrix Module Failure (SWMTXMOD) alarm occurs on the XC10G cross-connect card or a traffic card. If the alarm reports against a traffic card, it occurs when 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 card, it occurs when a logic component internal to the reporting cross-connect card is out of frame with a second logic component on the same cross-connect card. One or more traffic cards could lose traffic as a result of the cross-connect frame failure.

Clear the SWMTXMOD Alarm

Step 1 If the card reporting the alarm is the standby XC10G cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the standby cross-connect card.

Step 4 If the card reporting the alarm is the active cross-connect card, complete the "Side Switch the Active and Standby XC10G Cross-Connect cards" procedure on page 2-216.

Note After the active cross-connect goes into standby, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

Step 5 If the card reporting the alarm is not the active cross-connect card or if you completed the side switch in Step 4, complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 7 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the standby cross-connect card.

Step 8 If the card reporting the alarm is a traffic card, complete the "Side Switch the Active and Standby XC10G Cross-Connect cards" procedure on page 2-216.

Step 9 If the alarm does not clear after the cross-connect card side switch, complete the "Reset a Traffic Card in CTC" procedure on page 2-218 for the reporting card. For the LED behavior, see the "Non-DWDM Card LED Activity During Reset" section on page 2-212.

Step 10 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Step 11 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-219 for the traffic line card.

Step 12 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.295 SWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference (SWTOPRI) condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Note SWTOPRI is an informational condition. It does not require troubleshooting.

2.7.296 SWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference (SYNCSEC) 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.

Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-195.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.297 SWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference (SWTOTHIRD) 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.

Clear the SWTOTHIRD Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-195 or the "SYNCSEC" alarm on page 2-196.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.298 SYNC-FREQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The Synchronization Reference Frequency Out Of Bounds (SYNC-FREQ) condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Clear the SYNC-FREQ Condition

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency.

For specific procedures to use the test set equipment, consult the manufacturer. For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

Step 2 If the reference source frequency is not outside of bounds, complete the "Physically Replace a Card" procedure on page 2-219 for the TCC2 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 TCC2 to transfer the system software to the newly installed TCC2. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the TCC2 flash fail and then the active/standby LED flashes. When the transfer completes, the TCC2 reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ condition continues to report after replacing the TCC2 card, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.299 SYNCPRI

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

- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference (SYNCPRI) 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 on page 2-194.

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration for the REF-1 of the NE Reference.

Step 3 If the primary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-127.

Step 4 If the primary reference clock is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 5 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.300 SYNCSEC

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference (SYNCSEC) 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" alarm on page 2-194.

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration of the REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-127.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.301 SYNCTHIRD

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference (SYNCTHIRD) 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 TCC2 card may have failed. The ONS 15454 often reports either the "FRNGSYNC" condition on page 2-96 or the "HLDOVRSYNC" condition on page 2-104 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 at the lower-right outside edge of the shelf assembly.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify that the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-127.

Step 4 If the third timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 5 If the third timing source uses the internal ONS 15454 timing, complete the "Reset Active TCC2 Card and Activate Standby Card" procedure on page 2-217.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete "Remove and Reinsert (Reseat) the Standby TCC2" procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-219.

2.7.302 SYSBOOT

- Major (MJ), Service-Affecting (SA)
- Logical Object: NE

The System Reboot (SYSBOOT) alarm indicates that new software is booting on the TCC2 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.7.303 TIM

- Critical (CR), Service-Affecting (SA) for CLIENT, TRUNK
- Not Alarmed (NA), Non-Service Affecting (NSA) for OCN
- Logical Objects: CLIENT, OCN, TRUNK

The Section Trace Identifier Mismatch (TIM) alarm occurs when the expected J0 section trace string does not match the received section trace string.

If the condition occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Follow the procedure below to clear either instance.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (OCN)" alarm on page 2-132 or the "UNEQ-P" alarm on page 2-204. If these alarms accompany TIM, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm or Condition

Step 1 Log into the circuit source node and click the **Circuits** tab.

Step 2 Select the circuit reporting the condition, then click **Edit**.

Step 3 In 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 J1 Path Trace (port)** from the shortcut menu.

Step 5 Compare the Current Transmit String and the Current Expected String entries in the Edit J1 Path Trace dialog box.

Step 6 If the strings differ, correct the Transmit or Expected strings and click **Apply**.

Step 7 Click **Close**.

Step 8 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.304 TIM-MON

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The TIM Section Monitor Trace Identifier Mismatch (TIM-MON) alarm is similar to the "TIM-P" alarm on page 2-199, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when they are configured in transparent mode. (In Transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or vice versa.)

Clear the TIM-MON Alarm

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-199.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.305 TIM-P

- Critical (CR), Service-Affecting (SA) for STSTRM
- Minor (MN), Non-Service Affecting (NSA) for STSMON
- Logical Objects: STSMON, STSTRM

The TIM Path alarm (TIM-P) is raised when the expected SONET path trace string does not match the received path trace string.

The alarm is raised on an incoming SONET span card in the following sequence:

- A signal error occurs on a DS-1 or DS-3 electrical signal;
- The electrical card reports the error to the TCC2;
- The TCC2 determines that the error is on the SONET overhead instead of the electrical signal itself, and raises the alarm against the receiving SONET port.

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, type the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or a new, incorrect value has been entered in the Current Transmit String field. This procedure applies to either situation.

TIM-P also occurs on a port that has previously been operating without alarms if DS-3 cables or optical fibers connecting the ports are switched or removed. TIM-P is usually accompanied by other alarms, such as the "LOS (OCN)" alarm on page 2-132, the "UNEQ-P" alarm on page 2-204, or the "PLM-P" alarm on page 2-167. If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

Clear the TIM-P Alarm

Step 1 Complete the "Clear the TIM Alarm or Condition" procedure on page 2-198.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.306 TPTFAIL (FC_MR-4)

- Major (MJ), Service-Affecting (SA)
- Logical Object: FCMR

The Transport Fail (TPT-FAIL) alarm is raised against a local fibre channel (FC) port when the port receives another SONET error such as AIS-P, LOP-P, UNEQ-P, PLM-P, TIM-P, LOM (for VCAT only), or SQM (for VCAT only). This TPTFAIL can also be raised against fibre channel cards if the remote FC card port is down from INC-SIG-LOSS or INC-SYNC-LOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm).

Clear the TPTFAIL (FC_MR-4) Alarm

Step 1 Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.307 TPTFAIL (G1000)

- Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

The Transport (TPT) Layer Failure (TPTFAIL) alarm for the G-1000 Ethernet (traffic) cards 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 that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the "AIS-P" alarm on page 2-22, the "LOP-P" alarm on page 2-125, the "PDI-P" alarm on page 2-164, or the "UNEQ-P" alarm on page 2-204 exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 Ethernet port is administratively disabled or it is reporting the "CARLOSS (G1000)" alarm on page 2-46, the C2 byte in the SONET path overhead indicates the "PDI-P" alarm on page 2-164, which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS alarm to occur on the reporting port. In all cases, the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

Clear the TPTFAIL (G1000) 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. Clear any alarms being reported by the OC-N card on the G1000-4 circuit.

Step 2 If no alarms are reported by the OC-N card, or if the "PDI-P" condition on page 2-164 is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.7.308 TPTFAIL (ML100T, ML1000)

- Major (MJ), Service-Affecting (SA)
- Logical Objects: ML100T, ML1000

The TPT Layer Failure alarm for the ML100T or ML1000 Ethernet (traffic) cards indicates a break in the end-to-end POS link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the "AIS-P" condition on page 2-22, the "LOP-P" alarm on page 2-125, the "PDI-P" condition on page 2-164, or the "UNEQ-P" alarm on page 2-204 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML-Series POS port is administratively disabled, it inserts an "AIS-P" condition on page 2-22 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

Clear the TPTFAIL (ML100T, ML1000) Alarm

Step 1 If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.

Step 2 If the "PLM-P" alarm on page 2-167 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.

Step 3 If the "PDI-P" condition on page 2-164 is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a "CARLOSS (G1000)" alarm on page 2-46 is reported against the G-Series card, and if so, complete the "Clear the CARLOSS (G1000) Alarm" procedure on page 2-47.

Step 4 If the "AIS-P" alarm on page 2-22, the "LOP-P" alarm on page 2-125, or the "UNEQ-P" alarm on page 2-204 is present, clear those alarms using the procedures in those sections.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.309 TRMT

- Major (MJ), Service-Affecting (SA)

- Logical Object: DS1

A Missing Transmitter (TRMT) alarm occurs when there is a transmit failure on the DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 for the reporting DS-1 card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 an RMA.

2.7.310 TRMT-MISS

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Transmitter Missing (TRMT-MISS) alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector connects to a DS-1 card instead of a DS-3 card.

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

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the DS-1 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.311 TX-AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: DS1

The (TX) Transmit Direction AIS condition (TX-AIS) is raised by the ONS backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

Step 1 Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-132, or OOS ports.

Step 2 Clear the downstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.312 TX-RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The Transmit Direction RAI condition (TX-RAI) is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

Step 1 Complete the "Clear the TX-AIS Condition" procedure on page 2-203.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.313 UNC-WORD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Uncorrected FEC Word (UNC-WORD) condition indicates that the forward error correction (FEC) capability could not sufficiently correct the frame.

FEC allows the system to tolerate a 7- to 8 dB reduction in Signal to Noise Ratio (SNR).

Clear the UNC-WORD Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-180.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.314 UNEQ-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A signal label mismatch fault (SLMF) UNEQ Path alarm (UNEQ-P) occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from an incomplete circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note If you have created a new circuit but it has no signal, a UNEQ-P alarm is reported on the OC-N cards and the "AIS-P" condition on page 2-22 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 at the lower-right outside edge of the shelf assembly.

Clear the UNEQ-P Alarm

Step 1 In node view, click **View > Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel Circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7.

Step 6 If the Type column does contain VTT, attempt to delete these row(s):

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a. Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-217.

b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

c. If any other columns contain VTT, repeat Figure 2-1Step 6.

Step 7 If all ONS nodes in the ring appear in the CTC network view, determine whether the circuits are complete:

a. Click the **Circuits** tab.

b. Verify that INCOMPLETE is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as incomplete, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic.

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

Step 9 If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.

Complete the "Delete a Circuit" procedure on page 2-217.

Step 10 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide*.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a. Click the **Circuits** tab.

b. Verify that the Status column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *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 could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.**

Step 13 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-219 for the OC-N and 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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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 onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.315 UNEQ-V

- Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is 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.

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 could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified could 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 at the lower-right outside edge of the shelf assembly.

Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-204.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.316 VCG-DEG

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Degraded (VCG-DEG) alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the "OOU-TPT" alarm on page 2-157. It only occurs when a critical alarm, such as LOS, causes a signal loss.

Clear the VCG-DEG Condition

Step 1 Look for and clear any critical alarms that apply to the errored card, such as LOS (CLIENT), page 2-127 or LOS (OTS), page 2-134.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.317 VCG-DOWN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Down (VCG-DOWN) alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when both member circuits carried by the ML-Series Ethernet card are down. This alarm occurs in conjunction with another critical alarm, such as the "LOS (CLIENT)" alarm on page 2-127.

Clear the VCG-DOWN Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-207.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.318 VOA-HDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The variable optical attenuator (VOA) Degrade High alarm (VOA-HDEG) applies to amplifiers (OPT-BST and OPT-PRE), band add/drop cards (AD-1B-xx.x and AD-4B-xx), and to channel add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x) on the Line-1 TX port. It occurs when internal problem in the card keeps the VOA attenuation from maintaining the setpoint.

Clear the VOA-HDEG Alarm

Step 1 This alarm does not immediately affect traffic, but to clear the alarm, you will eventually need to complete the "Physically Replace a Card" procedure on page 2-219.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the *Cisco ONS 15454 SDH 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 condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.319 VOA-HFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Fail High alarm (VOA-HFAIL) occurs on OPT-BST and OPT-PRE amplifier cards when the amplifier VOA component is broken.

Clear the VOA-HFAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 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. Refer to the *Cisco ONS 15454 SDH 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 condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.320 VOA-LDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Degrade Low alarm (VOA-LDEG) applies to amplifiers (OPT-BST and OPT-PRE), band add/drop cards (AD-1B-xx.x and AD-4B-xx), and to channel add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x) on the Line-1 TX port. It occurs when internal problem in the card keeps the VOA attenuation from reaching the setpoint.

Clear the VOA-LDEG Alarm

Step 1 This alarm does not immediately affect traffic, but to clear the alarm, you will eventually need to complete the "Physically Replace a Card" procedure on page 2-219 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. Refer to the *Cisco ONS 15454 SDH 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 condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.321 VOA-LFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Fail Low alarm (VOA-LFAIL) occurs on OPT-BST and OPT-PRE amplifier cards when the amplifier VOA component is broken.

Clear the VOA-LFAIL Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-219 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. Refer to the *Cisco ONS 15454 SDH 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 condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.7.322 WKSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Working Switched To Protection (WKSWPR) condition occurs when a line experiences the "LOS (OCN)" alarm on page 2-132, the "SF (DS1, DS3)" condition on page 2-182, or the "SD (CLIENT, TRUNK)" condition on page 2-178.

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOS (OCN) Alarm" procedure on page 2-133.

Step 2 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.323 WTR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Wait To Restore (WTR) condition occurs when the "WKSWPR" condition on page 2-209 is raised the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic is switched back to the working path.

Caution DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.

Note WTR is an informational condition. It does not require troubleshooting.

2.7.324 WVL-MISMATCH

- Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Equipment Wavelength Mismatch (WVL-MISMATCH) alarm applies to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

Clear the WVL-MISMATCH alarm

Step 1 In node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card to display the card view.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 In the Wavelength field, view the provisioned card wavelength.

Step 4 If you have access to the site, compare the wavelength listed on the card faceplate with the provisioned wavelength. If you are remote, compare this wavelength with the card identification in the inventory:

a. In node view, click the **Inventory** tab.

b. Locate the slot where the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card is installed and view the card wavelength in the name.

Step 5 If the card was provisioned for the wrong wavelength, double-click the card in node view to display the card view.

Step 6 Click the **Provisioning > Card** tabs.

Step 7 In the Wavelength field, click the pull-down menu and choose the correct wavelength.

Step 8 Click **Apply**.

Step 9 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8 DS3-12 E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M13, or C Bit. The choice of framing format determines the line alarms that the DS3-12E card reports. The following table lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms as the standard DS-3 card.

Table 2-9 DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF	No	Yes	Yes
IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk	Yes	Yes	Yes
Facility Lpbk	Yes	Yes	Yes
FE Lpbk	No	No	Yes
FE Common Equipment Failure	No	No	Yes
FE Equipment Failure-SA	No	No	Yes
FE LOS	No	No	Yes
FE LOF	No	No	Yes
FE AIS	No	No	Yes
FE IDLE	No	No	Yes
FE Equipment Failure-NSA	No	No	Yes

2.9 DWDM and Non-DWDM Card LED Activity

DWDM cards and non-DWDM cards in the ONS 15454 system have somewhat different LED activity. The following sections list the LED behavior that occurs during card insertion, resetting, or in the case of the non-DWDM system, XC10G cross-connect card side-switching.

2.9.1 DWDM Card LED Activity After Insertion

When a DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.
6. The SF LED stays illuminated until all card ports connect to their far-end counterparts and a signal is present.

2.9.2 Non-DWDM Card LED Activity After Insertion

When a non-DWDM card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

2.9.3 DWDM Card LED Activity During Reset

When a DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.
2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters “LDG” appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

2.9.4 Non-DWDM Card LED Activity During Reset

While a non-DWDM card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters “LDG” appears on the reset card in CTC.

3. The green ACT LED appears in CTC.

2.9.5 Non-DWDM Cross-Connect LED Activity During Side Switch

While an XC10G cross-connect card is switched in CTC from active (ACT) to standby (SBY) or vice versa, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

2.9.6 Non-DWDM Card LED State After Successful Reset

When a non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials “SBY,” and this has replaced the white “LDG” depiction on the card in CTC.
- If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials “ACT,” and this has replaced the white “LDG” depiction on the card in CTC.

2.10 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*.

Identify a BLSR Ring Name 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 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

From the Ring Name column, record the ring name, or in the nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring Name

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > 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, enter the new name in the Ring Name field.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > 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**.

Verify Node Visibility for Other Nodes

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node 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**.

Verify or Create Node DCC Terminations

Note Portions of this procedure are different for DWDM.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > DCC/GCC/OSC** tabs.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

a. Click **Create**.

b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c. In the Port State area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Lock Out a BLSR Span

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node 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 Protect Span** and click **Apply**.

Step 5 Click **OK** on the BLSR Operations dialog box.

Clear a BLSR External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node 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.

Clear a Path Protection Lockout

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click **View > 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 In the Circuits on Span dialog box, choose **CLEAR** from the Perform UPSR Span Switching pull-down menu to remove a previously set switch command. Click **Apply**.

Step 5 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 6 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the switch state for all path protection circuits is CLEAR.

Switch Protection Group Traffic with an External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Display node view.

Step 3 Click the **Maintenance > Protection** tabs.

Step 4 Click the protection group that contains the reporting card.

Step 5 Click the Working or active card of the selected group.

Step 6 Click **Manual** and **Yes** in the confirmation dialog box.

Side Switch the Active and Standby XC10G Cross-Connect cards

Caution The cross-connect card side switch is traffic-affecting.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Display node view.

Step 3 Determine the active or standby XC10G cross-connect card.

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

Note You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the "Non-DWDM Cross-Connect LED Activity During Side Switch" section on page 2-213 for LED information.

Clear a Protection Group External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 Double-click the protection group that contains the reporting card.

Step 4 Highlight either selected group.

Step 5 Click **Clear** and click **Yes** in the confirmation dialog box.

Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Circuits** tab.

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** in the Delete Circuits dialog box.

Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback

Step 1 Log into a node on the network. If you are already logged in, continue with 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, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the pull-down menu and select None.

Step 6 In the State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the pull-down menu and select **IS**.

Step 8 Click **Apply**.

Reset Active TCC2 Card and Activate Standby Card

⚠ **Caution** The TCC2 card reset can be traffic-affecting.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active TCC2 card.

If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.

⚠ **Caution** Resetting an active TCC2 can cause data or provisioning loss if certain alarms—such as BKUPMEMP, CONTBUS-A-18, CONTBUS-B-18, CONTBUS-IO-A, CONTBUS-IO-B, DBOSYNC, DUP-IPADDR, DUP-NODENAME, HITEMP, I-HITEMP, MEM-GONE, PROTNA, SFTWDOWN, or SYSBOOT—are present and unresolved. Use the reset process only after resolving any of the named alarms. (You can use the procedure in the process of resolving the named alarms if instructed to do so.) If there is any doubt about whether the reset can cause data loss, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Step 3 Right-click the active TCC2 card in CTC.

Step 4 Choose **Reset Card** from the shortcut menu.

Step 5 Click **Yes** in the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "Non-DWDM Card LED State After Successful Reset" section on page 2-213.

Double-click the node and ensure that the reset TCC2 card is in standby mode and that the other TCC2 card is active.

- If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.
- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the active TCC2 ACT/SBY LED is green, and the LED of the standby TCC2 is amber.

Remove and Reinsert (Reseat) the Standby TCC2

Caution Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).

Caution The TCC2 card reseat can be traffic-affecting.

Note Before you reset the TCC2, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Ensure that the TCC2 you want to reset is in standby mode. On the TCC2 card, the ACT/SBY (Active/Standby) LED is amber when the TCC2 is in standby mode.

Step 3 When the TCC2 is in standby mode, unlatch both the top and bottom ejectors on the TCC2 card.

Step 4 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 5 Wait 30 seconds. Reinsert the card and close the ejectors.

Note The TCC2 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 TCC2 card reboots.

Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over Slots 1 to 4 and 14 to 17 or Slots 5, 6, 12, and 13 reporting the alarm.

Step 3 Right-click and choose **RESET CARD** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Verify BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

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

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column on the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

Step 5 If the entry is consistent with the original provisioning, go back to your original procedure.

Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

Step 7 Click **Apply**.

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. See the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-216 for more 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.

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.

Remove and Reinsert Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15454.

Step 3 Close the retractable handles.

CHAPTER 3

Replace Hardware

This chapter provides procedures for replacing Cisco ONS 15454 hardware.

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

Chapter includes the following sections:

1. 3.1 Replace an In-Service Cross-Connect Card, page 3-2—Complete this procedure to replace an in-service cross-connect card.
2. 3.2 Replace the Air Filter, page 3-5—Complete this procedure to replace a reusable or disposable air filter.
3. 3.3 Determine Fan-Tray and AIP Replacement Compatibility, page 3-9—Complete this procedure to verify replacement hardware compatibility.
4. 3.4 Replace the Fan-Tray Assembly, page 3-10—Complete this procedure to replace the fan-tray assembly.
5. 3.5 Replace the Alarm Interface Panel, page 3-12—Complete this procedure to replace the alarm interface panel (AIP).
6. 3.6 Replace an Electrical Interface Assembly, page 3-17—Complete this procedure to replace the electrical interface assembly (EIA).
7. 3.8 Replace the Small Form-Factor Pluggable Connector, page 3-19—Complete this procedure as needed to replace the small form-factor pluggable (SFP) connector used with ML-Series Ethernet cards.
8. 3.9 Install the Plastic Lower Backplane Cover, page 3-19—Complete this procedure as needed to replace the metal lower backplane cover with a plastic lower backplane cover.

3.1 Replace an In-Service Cross-Connect Card

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

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 when a card reseat is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card replacement is complete.

In a bidirectional line switched ring (BLSR), path protection, or 1+1 configuration, pulling the active cross-connect card (XC/XCVT/XC10G) without a lockout might cause circuits to switch. Therefore, you must inhibit protection switching before replacing the in-service cross-connect card.

Step 1 Log into the node where you will replace the card. For login procedures, see the *Cisco ONS 15454 Procedure Guide*.

Step 2 Ensure that the working span is active on both local and remote nodes. The purpose of verifying the active span is to know which one to lock out:

a. In node 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 that the working span is carrying error-free traffic (no signal degrade [SD] or signal fail [SF] alarms present). Display the network view and click the **Alarms** tab to display alarms and to make sure that no alarm filters are applied.

Step 4 Lock out or switch the protection span according to the network topology. To lock out a BLSR, go to Step 5. To lock out a protection span in a 1+1 protection scheme, go to Step 6. To switch path protection traffic, go to Step 7.

Step 5 Lock out the protection span in a BLSR protection scheme:

a. In node view, click the **Provisioning > BLSR** tabs.

b. Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

c. To lock out a west span:

- Right-click any BLSR node west channel (port) and choose **Set West Protection Operation**.

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. You can right-click either working port.

- In the Set West Protection Operation dialog box, choose **LOCKOUT SPAN** from the drop-down menu. Click **OK**.
- In the Confirm BLSR Operation dialog box, click **Yes**. An “L” indicating the lockout appears on the selected channel (port) where you created the lockout.

  Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

d. To lock out an east span:

- Right-click the node’s east channel (port) and choose **Set East Protection Operation**.
- In the Set East Protection Operation dialog box, choose **LOCKOUT SPAN** from the drop-down menu. Click **OK**.
- In the Confirm BLSR Operation dialog box, click **Yes**. An “L” indicating the lockout appears on the selected channel (port) where you invoked the protection switch.

  Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.
- From the File menu, choose **Close**.

Step 6 To lock out a protection span in a 1+1 protection scheme:

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

b. Under Protection Groups, click the protection group that contains the card you want to lock out.

c. Under Selected Group, click the card you want to lock out.

d. From Inhibit Switching, click **Lock Out**.

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

The lockout has been applied and traffic is switched to the opposite card.

Note Provisioning a lockout causes a LOCKOUT-REQ or an FE-LOCKOUT condition to be raised on CTC. Clearing the lockout switch request clears these conditions; they are informational only.

Step 7 To Force switch traffic in a path protection scheme:

- In node view, choose **Go to Network View**.
- Right-click the span where you want to switch path protection traffic away. Choose **Circuits** from the shortcut menu.
- In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.
- In the Confirm UPSR Switch dialog box, click **Yes**.
- In the Protection Switch Result dialog box, click **OK**.

  In the Circuits on Span window, the Switch State for all circuits is Force.

Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the Force switch; it is informational only.

Step 8 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 9 Switch the active cross-connect card (XC/XCVT/XC10G) to standby:

a. In the node view, click the **Maintenance > XC Cards** tabs.

b. Under Cross Connect Cards, choose **Switch**.

c. Click **Yes** in 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 10 Physically remove the new standby cross-connect card (XC/XCVT/XC10G) from the ONS 15454.

Step 11 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 12 Release the lockout of the protection span in a BLSR protection scheme (if one was applied in Step 4):

a. In node view, click the **Provisioning > BLSR** tabs.

b. Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

c. Right-click the BLSR node channel (port) where the lockout will be cleared and choose **Set West Protection Operation** or **Set East Protection Operation**.

d. In the dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

e. In the Confirm BLSR Operation dialog box, click **Yes**. The “L” indicating the lockout is removed from the network view map.

f. From the File menu, choose **Close**.

Step 13 Release the lockout of the protection span in a 1+1 protection scheme (if one was applied in Step 4):

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

b. Under Protection Groups, click the protection group that contains the card you want to clear.

c. Under Selected Group, click the card you want to clear.

d. From Inhibit Switching, click **Unlock**.

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

Step 14 Clear the Force switch for the path protection scheme (if one was applied in Step 4):

a. In node view, choose **Go to Network View**.

b. Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

c. In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.

d. In the Confirm UPSR Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

f. In the Circuits on Span window, the Switch State for all path protection circuits is CLEAR.

The lockout is cleared.

3.2 Replace the Air Filter

Inspect the air filters every 30 days and clean as needed.

3.2.1 Inspect, Clean, and Replace the Reusable Air Filter

You need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

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

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 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 might 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. If it is already open or if the shelf assembly does not have a front door, continue with Step 3.

- Open the front door lock.

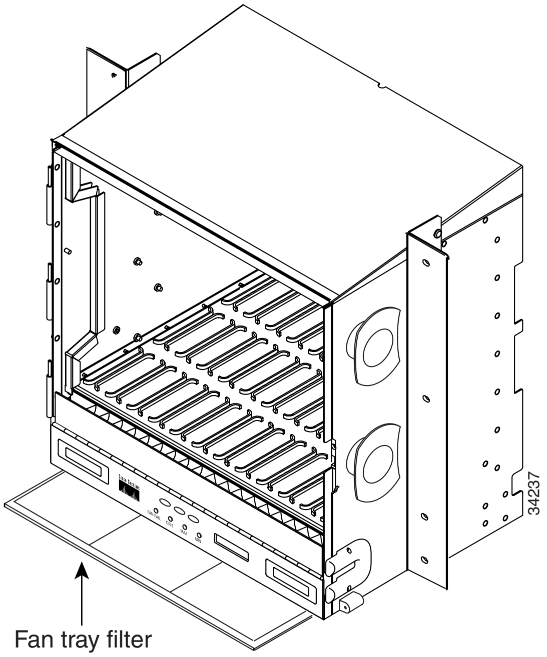
  The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

- 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 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 (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 5 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 6 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.

Step 7 Visually inspect the air filter material for dirt and dust.

Step 8 If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.

Caution Do not put a damp filter back in the ONS 15454.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

Note On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

Step 14 Replace the door and reattach the ground strap.

3.2.2 Inspect and Replace the Disposable Air Filter

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. If the shelf assembly does not have a front door, continue with Step 4.

a. 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.

b. Press the door button to release the latch.

c. Swing the door open.

Step 3 Remove the front door (optional). If you do not want to remove the door, proceed to Step 4.

a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

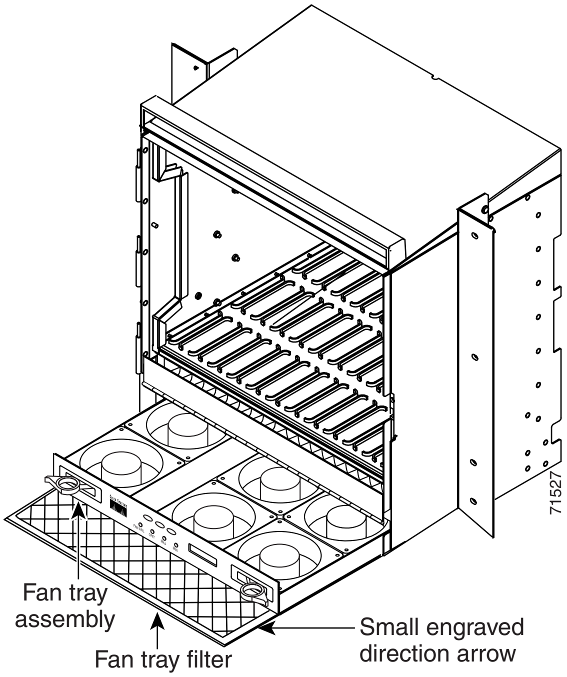
c. Secure the dangling end of the ground strap to the door or chassis with tape.

Step 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 (25.4 mm) out of the shelf assembly and wait until the fans stop.

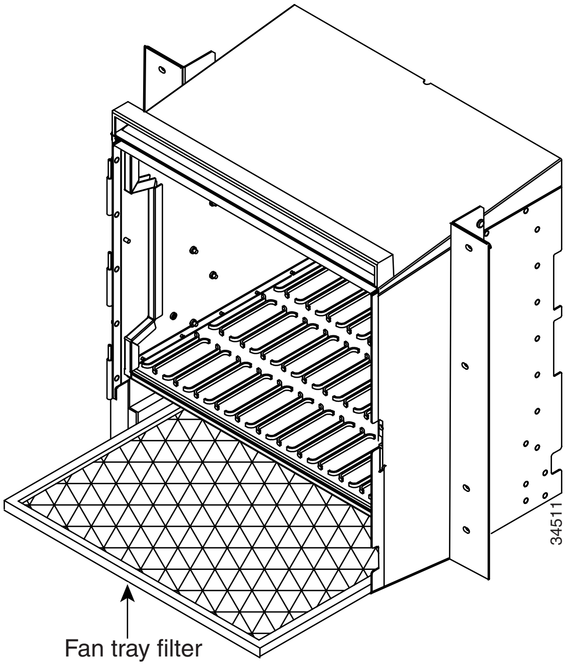
Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 3-2).

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 might have collected on the filter.

Figure 3-3 Inserting or Removing a Disposable Fan-Tray Air Filter (Front Door Removed)



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.

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 Replace the door and reattach the ground strap.

3.3 Determine Fan-Tray and AIP Replacement Compatibility

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;15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.

Note The 15454-SA-ANSI or 15454-SA-HD 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 that you have compatible components when replacing the fan-tray assembly or the AIP and note the alarms that will occur when an incompatibility occurs.

Note If you need to determine the hardware that has been installed on a node, click the inventory tab in node view.

Table 3-1 Incompatibility Alarms

Shelf Assembly [1]	Fan Tray[2]	AIP[3]	10G Cards[4]	Ethernet Cards[5]	Alarms
—	—	No fuse	—	—	Mismatch of Equipment Attributes (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

Table 3-1 Incompatibility Alarms (continued)

Shelf Assembly [1]	Fan Tray[2]	AIP[3]	10G Cards[4]	Ethernet Cards[5]	Alarms
ANSI or HD	2A	2A	No	—	None
ANSI or HD	2A	2A	Yes	2.5G compatible	MEA on fan tray, AIP, Ethernet
ANSI or HD	2A	2A	Yes	10G compatible	MEA on fan tray, AIP
ANSI or HD	2A	5A	No	Either	None
ANSI or HD	2A	5A	Yes	2.5G compatible	MEA on fan tray, Ethernet
ANSI or HD	2A	5A	Yes	10G compatible	MEA on fan tray
ANSI or HD	5A	2A	No	Either	MEA on AIP
ANSI or HD	5A	2A	Yes	2.5G compatible	MEA on AIP, Ethernet
ANSI or HD	5A	2A	Yes	10G compatible	MEA on AIP
ANSI or HD	5A	5A	No	Either	None
ANSI or HD	5A	5A	Yes	Either	None

[1] 15454-SA-ANSI (P/N: 800-19857-01) = ONS 15454 Release 3.1 and later shelf assembly,
15454-SA-HD (P/N: 800-24848) = 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

[2] 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)

[3] 5A AIP (P/N: 73-7665-01), 2A AIP (P/N: 73-5262-01)

[4] 10G cards = XC-10G, OC-192, OC-48 AS

[5] 2.5G compatible Ethernet cards = E1000-T, E1000-2, E1000T-G, E10002-G, G1000-4, G1K-4
10G compatible Ethernet cards = E1000T-G, E10002-G, G1000-4, G1K-4, ML100T-12, ML1000-2

Step 2 See the "3.4 Replace the Fan-Tray Assembly" section on page 3-10 to replace the fan-tray assembly or the "3.5 Replace the Alarm Interface Panel" section on page 3-12 to replace the AIP.

3.4 Replace the Fan-Tray Assembly

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a 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 backplane.

Note The 15454-SA-ANSI or 15454-SA-HD 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.

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

Step 1 Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with Step 3.

a. 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.

b. Press the door button to release the latch.

c. Swing the door open.

Step 2 Remove the front door (optional). If you do not want to remove the door, proceed to Step 3.

a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

c. Secure the dangling end of the ground strap to the door or chassis with tape.

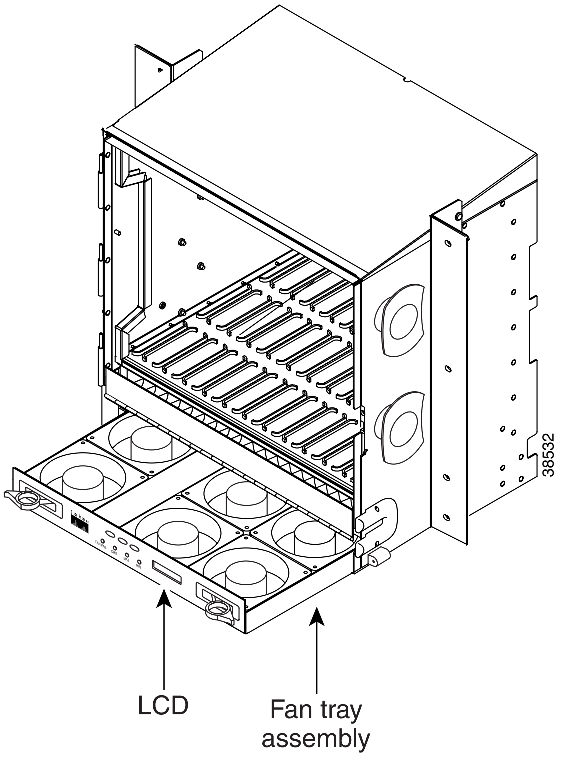
Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Fold out the retractable handles at the outside edges of the fan tray.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. Figure 3-4 shows the location of the fan tray.

Figure 3-4 Removing or Replacing the Fan-Tray Assembly (Front Door Removed)



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 "3.2 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, be sure to reattach the ground strap.

3.5 Replace the Alarm Interface Panel

⚠ **Caution** Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.

⚠ **Caution** If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Assistance Center (TAC) at 1 800 553-2447 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 during a maintenance window. Resetting the active TCC2 card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC2 card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Caution Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC (1 800 553-2447).

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 will be affected.

You need a #2 Phillips screwdriver.

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

a. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.

b. If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.

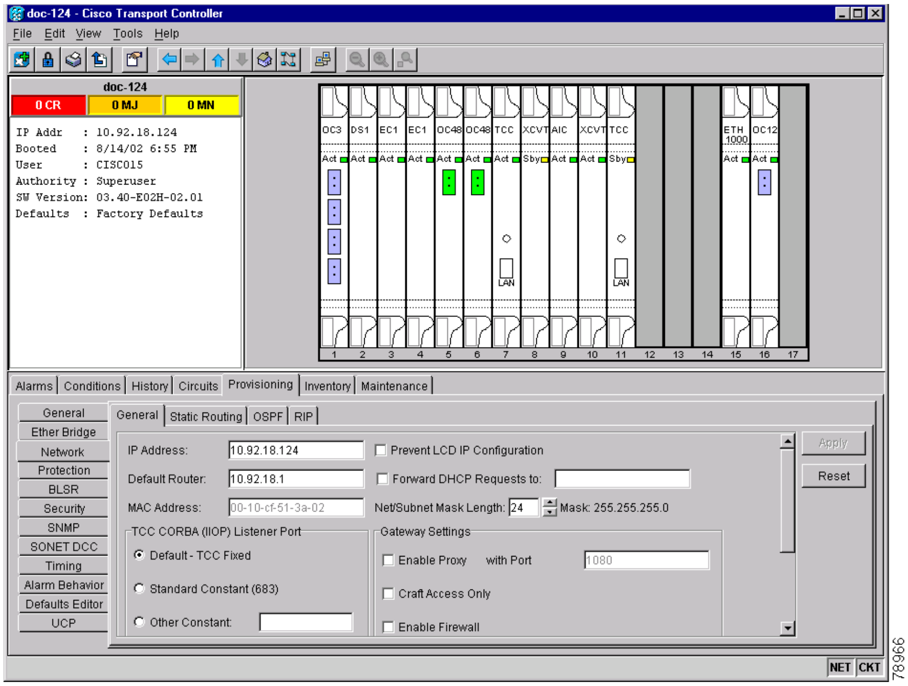
Step 2 Record the MAC address of the old AIP:

a. Log into the node where you will replace the AIP. For login procedures, see the *Cisco ONS 15454 Procedure Guide*.

b. In node view, click the **Provisioning > Network** tabs.

c. Record the MAC address shown in the General tab (Figure 3-5).

Figure 3-5 Find the MAC Address


doc-124 - Cisco Transport Controller

doc-124
0 CR 0 MJ 0 MN

```
IP Addr   : 10.92.18.124
Booted    : 8/14/02 6:55 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

IP Address: 10.92.18.124 □ Prevent LCD IP Configuration

Default Router: 10.92.18.1 □ Forward DHCP Requests to:

MAC Address: 00-10-cf-51-3a-02 Net/Subnet Mask Length: 24 Mask: 255.255.255.0

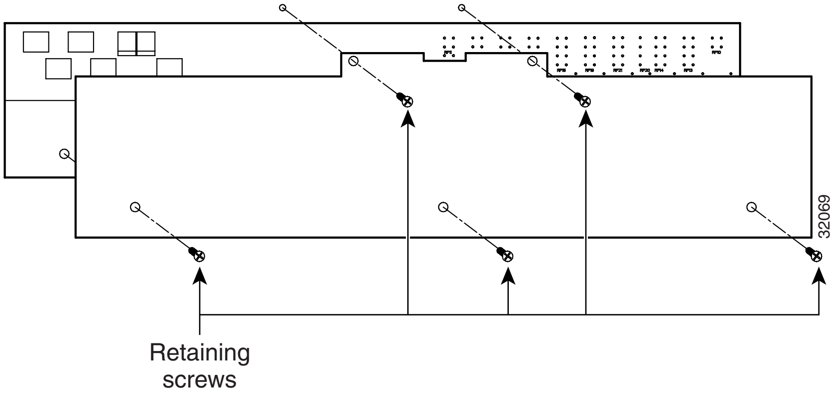
TCC CORBA (IIOP) Listener Port
● Default - TCC Fixed
○ Standard Constant (683)
○ Other Constant:

Gateway Settings
□ Enable Proxy with Port 1080
□ Craft Access Only
□ Enable Firewall

Step 3 Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place (Figure 3-6).

Figure 3-6 Lower Backplane Cover



Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848); doing so will cause a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning > Network** tabs.

Caution Cisco recommends TCC2 card resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby TCC2 card:

a. Right-click the standby TCC2 card and choose **Reset Card**.

b. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.

Note The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active TCC2 card:

a. Right click the active TCC2 card and choose **Reset Card**.

b. Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication will appear on the card in CTC.

Note The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down menu choose **Exit** to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down menu.

Step 20 Record the new MAC address:

a. In node view, click the **Provisioning > Network** tabs.

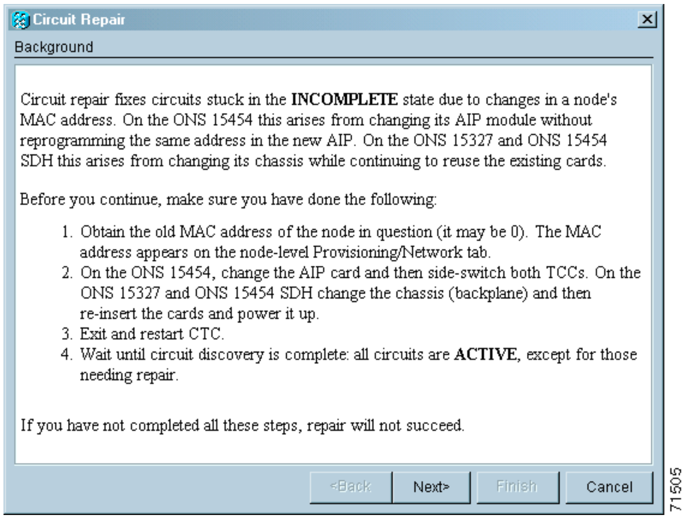
b. Record the MAC address shown in the General tab.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are in an INCOMPLETE state.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down menu. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box (Figure 3-7). If all the steps in the dialog box have been completed, click **Next>**. Ensure that you have the old and new MAC addresses.

Figure 3-7 Repairing Circuits



Circuit Repair

Background

Circuit repair fixes circuits stuck in the **INCOMPLETE** state due to changes in a node's MAC address. On the ONS 15454 this arises from changing its AIP module without reprogramming the same address in the new AIP. On the ONS 15327 and ONS 15454 SDH this arises from changing its chassis while continuing to reuse the existing cards.

Before you continue, make sure you have done the following:

1. Obtain the old MAC address of the node in question (it may be 0). The MAC address appears on the node-level Provisioning/Network tab.
2. On the ONS 15454, change the AIP card and then side-switch both TCCs. On the ONS 15327 and ONS 15454 SDH change the chassis (backplane) and then re-insert the cards and power it up.
3. Exit and restart CTC.
4. Wait until circuit discovery is complete: all circuits are **ACTIVE**, except for those needing repair.

If you have not completed all these steps, repair will not succeed.

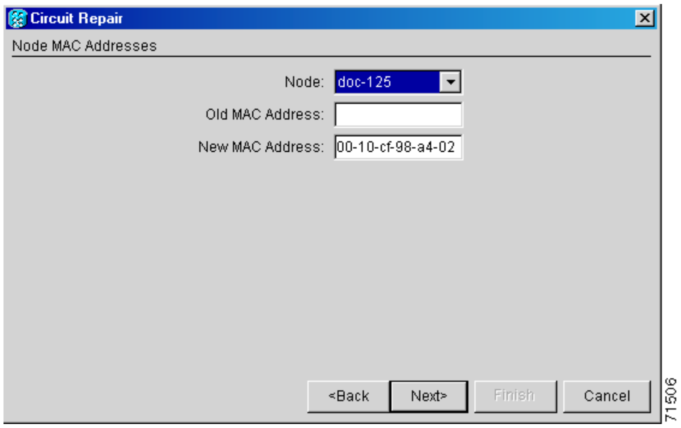
Step 24 The Node MAC Addresses dialog box appears (Figure 3-8):

a. From the Node drop-down menu, choose the name of the node where you replaced the AIP.

b. In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.

c. Click **Next**.

Figure 3-8 Recording the Old MAC Address Before Replacing the AIP



Circuit Repair

Node MAC Addresses

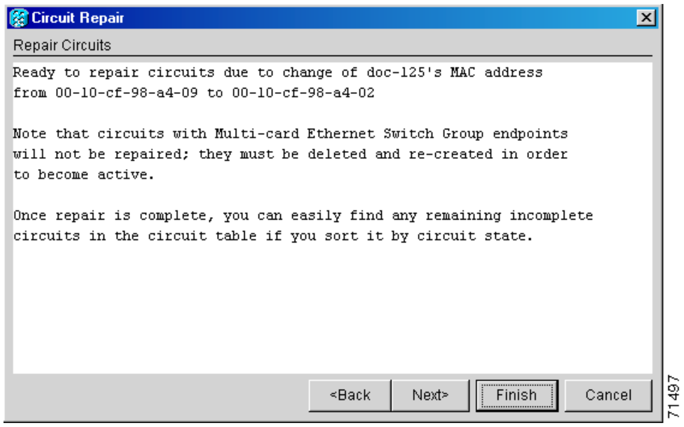
Node: doc-125

Old MAC Address:

New MAC Address: 00-10-cf-98-a4-02

Step 25 The Repair Circuits dialog box appears (Figure 3-9). Read the information in the dialog box and click **Finish**.

Figure 3-9 Circuit Repair Information



```
Ready to repair circuits due to change of doc-125's MAC address
from 00-10-cf-98-a4-09 to 00-10-cf-98-a4-02

Note that circuits with Multi-card Ethernet Switch Group endpoints
will not be repaired; they must be deleted and re-created in order
to become active.

Once repair is complete, you can easily find any remaining incomplete
circuits in the circuit table if you sort it by circuit state.
```

Note The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, 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 the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).

3.6 Replace an Electrical Interface Assembly

You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

Step 1 To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 3-6 on page 3-14).

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 it away from the backplane.

Note Attach backplane sheet metal covers whenever EIAs are not installed.

Step 5 Line up the connectors on the new EIA with the mating connectors on the backplane.

Step 6 Gently push the EIA until both sets of connectors fit together snugly.

Step 7 Replace the nine perimeter screws that you removed while removing the backplane cover.

Step 8 If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

Step 9 Reattach the lower backplane cover.

3.7 Replace the Gigabit Interface Converter

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

Step 2 If you are using a GBIC with clips:

a. Release the GBIC from the slot by squeezing the two plastic tabs on each side of the GBIC.

b. Slide the GBIC out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Step 3 If you are using a GBIC with a handle:

a. Release the GBIC by opening the handle.

b. Pull the handle of the GBIC.

c. Slide the GBIC out of the Gigabit Ethernet card slot. A flap closes over the GBIC slot to protect the connector on the Gigabit Ethernet card.

Step 4 Remove the new GBIC or SFP from its protective packaging if necessary.

Step 5 Check the label to verify that the GBIC or SFP is the correct type for your network.

Refer to the *Cisco ONS 15454 Procedure Guide* for a list of applicable part numbers.

Step 6 Verify the type of GBIC or SFP you are using:

- If you are using a GBIC with clips, go to Step 7.
- If you are using a GBIC with a handle, go to Step 8.

Step 7 For GBICs with clips:

a. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

Note GBICs are keyed to prevent incorrect installation.

b. Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

c. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

d. Proceed to Step 8.

Step 8 For GBICs with a handle:

a. Remove the protective plug from the SC-type connector.

b. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

c. Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to an SC-type connector.

d. Slide the GBIC through the cover flap until you hear a click.

The click indicates that the GBIC is locked into the slot.

3.8 Replace the Small Form-Factor Pluggable Connector

Step 1 Unplug the SFP connector and fiber from the ML-Series Ethernet card or Muxponder (MXP) card.

Step 2 If the SFP connector has a latch securing the fiber-optic cable, pull it upward to release the cable.

Step 3 Pull the fiber cable straight out of the connector.

Step 4 Plug the fiber into a Cisco-supported SFP connector.

Step 5 If the new SFP connector has a latch, close the latch over the cable to secure it.

Step 6 Plug the cabled SFP connector into the ML-Series Ethernet card port or Muxponder port until it clicks.

3.9 Install the Plastic Lower Backplane Cover

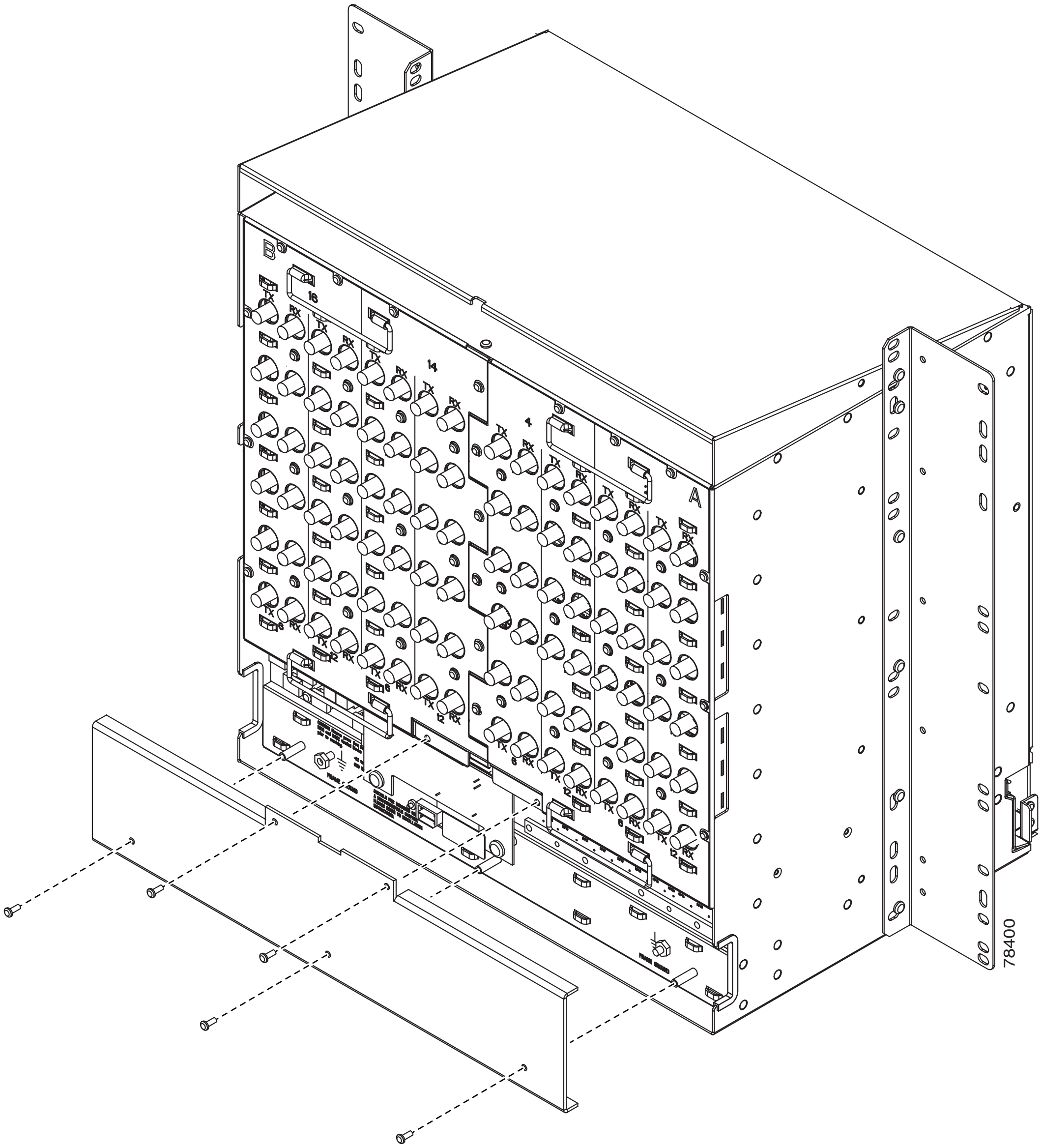
Step 1 Unscrew the five retaining screws that hold the metal cover in place.

Step 2 Grasp the metal cover on each side.

Step 3 Gently pull the metal cover away from the backplane.

Step 4 Place the plastic cover against the shelf assembly and align the screw holes on the cover and the shelf assembly (Figure 3-10).

Figure 3-10 Attaching Plastic Lower Backplane Cover



Step 5 Tighten the five retaining screws that hold the plastic cover in place.

CHAPTER 4

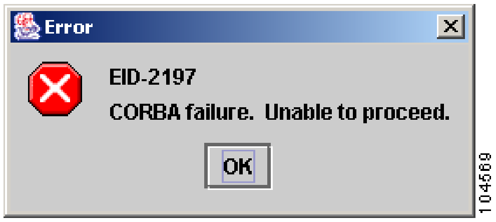
Error Messages

This chapter lists the ONS 15454 error messages. Error message numbering is a new feature in Release 4.6. Table 4-1 gives a list of all error message numbers, the messages, and a brief description of each message.

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

The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and the error message.

Figure 4-1 Error Dialog Box


Error

EID-2197

CORBA failure. Unable to proceed.

Table 4-1 Error Messages

Error ID	Error Message	Description
EID-0000	Invalid Error ID.	The error ID is invalid.
EID-0001	Null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to error message text.
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and re-start your browser in order for the new permissions to take effect.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	Refer to error message text.
EID-1003	General exception. {0}	Unexpected exception/error while launching CTC from the applet. Failed to rollback card provisioning while cancelling a span upgrade. Unexpected error while assigning east or west protect port of a bidirectional line switched ring (BLSR).

EID-1004	Problem Deleting CTC Cache:
	{0}
	{1}
		CTC encountered a problem deleting the cache.

EID-1005	IOException writing batch file to launch CTC.	CTC could not write the launching batch file.
EID-1006	Malformed URL trying to download LAUNCHER.jar.	The URL used to download the Launcher.jar file is malformed.
EID-1007	IO Exception trying to download LAUNCHER.jar.	An input/output exception was encountered when CTC tried to download the GUI launcher.
EID-1008	Malformed URL trying to download ORB.	The URL used to download the ORB.jar file is malformed.
EID-1009	IO Exception trying to download ORB.	There was a problem trying to download the ORB.jar file. It has not been downloaded.
EID-1010	Alias Exists.	The alias already exists.
EID-1011	KeyStoreException	CTC encountered a keystore exception trying to complete this task.
EID-1012	Can not find file. FileNotFoundException	The file could not be found.
EID-1013	IOException	CTC encountered an input/output exception.
EID-1014	NoSuchAlgortihmException	The algorithm does not exist.
EID-1015	CertificateException	CTC encountered a certificate exception.
EID-1016	Null Keystore	CTC encountered a null keystore while trying to complete this task.
EID-1017	The policy file was not changed due to an error writing the {0} file.	The policy file was not changed due to an error writing the specified file.
EID-1018	Password must contain at least 1 alphabetic, 1 numeric, and 1 special character (+, # or %). Password shall not contain the associated user-ID	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename to save file as.	CTC could not create the file due to an invalid filename.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-1020	Fatal exception occurred, exiting CTC. Unable to switch to the Network view.	CTC was unable to switch from the node or card view to the network view, and is now shutting down.
EID-1021	Unable to navigate to {0}.	Failed to display the indicated view—node or network.
EID-1022	A session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to error message text.
EID-1023	This session has been terminated. This can happen if the card resets, the session has timed out, or if someone else (possibly using a different CTC) already has a session open with this slot.	Refer to error message text.
EID-1024	Error writing to {0}.	An error occurred while exporting an HTML report.
EID-1025	Unable to create Help Broker	CTC was unable to create the help broker for the online help.
EID-1026	Unable to locate HelpSet.	CTC was unable to locate the help set for the online help.
EID-1027	Unable to locate Help ID: {0}	CTC was unable to locate the help ID for the online help.
EID-1028	Error saving table {0}.	There was an error saving the specified table.
EID-1029	Malformed URL trying to download {0}.jar.	The URL used to download the JavaHelp JAR file is malformed.
EID-1030	IO Exception trying to download {0}.jar.	An input/output error occurred while CTC was downloading the specified JAR file.
EID-2001	No rolls selected.	No rolls were selected for the bridge and roll.
EID-2002	The Roll must be completed or cancelled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	Error deleting roll.	There was an error when CTC tried to delete the roll.
EID-2004	No IOS slot selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files may have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.	CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.
EID-2006	Error editing circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	Unable to save preferences.	CTC cannot save the preferences.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2008	Unable to store circuit preferences. File not found.	CTC cannot find the file needed to save the circuit preferences.
EID-2009	Unable to store circuit preferences. I/O error.	An input/output error is preventing CTC from saving the circuit preferences.
EID-2010	Delete destination failed.	CTC could not delete the destination.
EID-2011	Circuit destroy failed.	CTC could not destroy the circuit.
EID-2012	Reverse circuit destroy failed.	CTC could not reverse the circuit destroy.
EID-2013	Circuit creation error. Circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog will close. Please try again.	Refer to error message text.
EID-2014	No circuit(s) selected.	You must select a circuit to complete this function.
EID-2015	Cannot delete circuit. {0}	CTC cannot delete the circuit.
EID-2016	Circuit deletion error.	There was an error deleting the circuit.
EID-2017	Error mapping circuit. {0}	There was an error mapping the circuit.
EID-2018	Circuit roll failure. The circuit has to be in the ACTIVE state in order to perform a roll.	Refer to error message text.
EID-2019	Circuit roll failure. The current version does not support bridge and roll on a VT tunnel.	Refer to error message text.
EID-2020	Circuit roll failure. The two circuits must have the same direction.	Refer to error message text.
EID-2021	Circuit roll failure. The two circuits must have the same size.	Refer to error message text.
EID-2022	Circuit roll failure. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to error message text.
EID-2023	Error deleting circuit. {0}	There was an error deleting the circuit.
EID-2024	Node selection error.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each of the endpoints of this circuit are running software that supports this feature.	This error is generated from the AnsOpticsParamsPane to indicate that the selected ring type is not supported by the endpoints of the circuit. In the VLAN pane it indicates that the backend spanning tree protocol (STP) disabling is not supported.
EID-2026	Request failed. {0}	Error occurred while attempting to switch a path protection circuit away from a span.
EID-2027	Error deleting circuit drop.	CTC could not delete the circuit drop.
EID-2028	Error removing circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2030	Provisioning error.	There was an error during provisioning.
EID-2031	Error adding node.	There was an error while adding a node.
EID-2032	Error renaming circuit. {0}	CTC could not rename the circuit.

EID-2033	Cannot verify table data.
	{0}
	{1}
		There was an internal error while validating the user changes during Apply. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).

EID-2034	Cannot verify table data. {0}	There was an internal error while validating the user changes during Apply. This error occurs in the Edit Circuit dialog box.
EID-2035	The source and destination nodes are not connected.	Refer to error message text.
EID-2036	Error deleting circuit drop.	There was an error deleting the circuit drop.
EID-2037	Application error. Cannot find attribute for {0}.	CTC cannot find an attribute for the specified item.
EID-2038	Invalid protection operation.	There was an invalid protection operation.
EID-2039	Internal communication error.	CTC experienced an internal communication error.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	Refer to error message text.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to error message text.
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path.	Refer to error message text.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to error message text.
EID-2046	No paths are available on this link. Please make another selection.	Refer to error message text.
EID-2047	Error validating slot number. Please enter a valid value for the slot number.	Refer to error message text.
EID-2048	Error validating port number. Please enter a valid value for the port number.	Refer to error message text.
EID-2049	Delete destination failed.	CTC could not delete the destination.
EID-2050	New circuit destroy failed.	CTC could not destroy the new circuit.
EID-2051	Circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2052	Error during circuit processing.	There was an error during the circuit processing.
EID-2053	No rolls selected. {0}	You did not select a roll for this task.
EID-2054	Endpoint selection error.	There was an error during the endpoint selection.
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race conditionthat has incorrectly allowed entities without endpoints to be displayed in the combo boxes.
EID-2056	Communication error.	An internal error occurred while synchronizing alarms with the nodes. Network Alarm pane.
EID-2058	Node deletion error. {0}	There was an error during the node deletion.
EID-2059	Node deletion Error. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	Error defining VLAN.	There was an error defining the VLAN.
EID-2062	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.
EID-2063	Cannot delete default VLAN.	The selected VLAN is the default VLAN, and cannot be deleted.
EID-2064	Error deleting VLANs. {0}	There was an error deleting the VLAN.
EID-2065	Cannot import profile. Profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.	Cannot import profile. The specified profile exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.
EID-2066	Unable to store profile. Error writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	File write error. {0}	CTC encountered a file write error.
EID-2068	ProvAlarmsPanedoImportNode error.	CTC encountered a ProvAlarmsPanedoImportNode error.
EID-2069	File not found or I/O exception. {0}	Either the file was not found, or there was an input/output exception.
EID-2070	Failure deleting profile. {0}	The profile deletion failed.
EID-2071	Only one column may be highlighted.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2072	Only one profile may be highlighted.	Refer to error message text.
EID-2073	This column is permanent and may not be removed.	Refer to error message text.
EID-2074	Select one or more profiles.	Refer to error message text.
EID-2075	This column is permanent and may not be reset.	Refer to error message text.
EID-2076	Error in reset refresh. {0}	CTC encountered an error during the view reset/refresh.
EID-2077	This column is permanent and may not be renamed.	Refer to error message text.
EID-2078	At least two columns must be highlighted.	Refer to error message text.
EID-2079	Cannot load alarmables into table. There are no reachable nodes from which the list of alarmables may be loaded. Please wait until such a node is reachable and try again.	Refer to error message text.
EID-2080	Node {0} does not have deletable profiles.	The specified node does not have any deletable profiles.
EID-2081	Error removing profile {0} from node {1}.	There was an error removing the specified profile from the node.
EID-2082	Cannot find profile {0} on node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	Error adding profile {0} to node {1}.	There was an error adding the specified profile to the specified node.
EID-2084	Node {0} has no profiles.	The specified node has no profiles.
EID-2085	Invalid profile selection. No profiles were selected.	Refer to error message text.
EID-2086	Invalid node selection. No nodes were selected.	Refer to error message text.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to error message text.
EID-2088	Invalid profile name.	Refer to error message text.
EID-2089	Too many copies of {0} exist. Please choose another name.	Too many copies of the specified item exist.
EID-2090	No nodes selected. Please select the node(s) on which to store the profile(s).	Refer to error message text.
EID-2091	Unable to switch to node {0}.	CTC is unable to switch to the specified node.
EID-2092	General exception error.	CTC encountered a general exception error while trying to complete the task.
EID-2093	Not enough characters in name. {0}	There are not enough characters in the name.
EID-2094	Password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	Illegal password. {0}	The password you entered is not allowed.
EID-2096	The user must have a security level.	You must have an assigned security level to perform this task.
EID-2097	No user name specified.	You did not specify a user name.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2098	Ring switching error.	There was an error during the ring switch.
EID-2099	Ring switching error.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	Refer to error message text.
EID-2101	Protection switching error.	There was an error during the protection switch.
EID-2102	{0} The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	Span upgrade error.	There was an error during the span upgrade.
EID-2104	Unable to switch circuits back as one or both nodes are not reachable.	This error occurs during the path protection span upgrade procedure.
EID-2105	Span upgrade error.	There was an error during the span upgrade.
EID-2106	The node name cannot be empty.	You must supply a name for the node.
EID-2107	Error adding {0}, unknown host.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item is already in the network.
EID-2109	The node is already in the current login group.	Refer to error message text.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Refer to error message text.
EID-2112	You must enter a number and it must be between 0 and {0}.	You must enter a number and it must be between 0 and the specified number.
EID-2113	Cannot set extension byte. {0}	CTC cannot set the extension byte.
EID-2114	Card communication failure. Error applying operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	Error applying operation. {0}	There was an error applying the specified operation.
EID-2116	Invalid extension byte setting. {0}	The extension byte set is invalid.
EID-2118	Cannot delete ring. There is a protection operation set. All protection operations must be clear for ring to be deleted.	Refer to error message text.
EID-2119	Cannot delete {0} because a protection switch is in effect. Please clear any protection operations, make sure that the reversion time is not "never" and allow any protection switches to clear before trying again.	Refer to error message text.
EID-2120	The following nodes could not be unprovisioned {0} Therefore you will need to delete this {1} again later.	The specified nodes could not be unprovisioned.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2121	Cannot upgrade ring. {0}	CTC cannot upgrade the ring.
EID-2122	Inadequate ring speed for upgrade. Only {0} (or higher) {1} can be upgraded to 4-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber.
EID-2123	Non-upgradable nodes. Verify that the following nodes have at least two in-service ports with the same speed as the 2-fiber {0}. The ports cannot serve as a timing reference, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two in-service ports with the same speed as the 2-fiber. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to error message text.
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to error message text.
EID-2126	OSPF area error.	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause some circuits to occupy different STS regions on different spans.	Refer to error message text.
EID-2128	Illegal state error.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	This port is already assigned. The east and west ports must be different.	Refer to error message text.
EID-2130	The ring ID value is not valid. Please enter a valid number between 0 and 9999.	Refer to error message text.
EID-2131	Cannot set reversion to INCONSISTENT.	You must select another reversion type.
EID-2132	Invalid ring ID. {0}	The ring ID you entered is invalid. Please use another ID.
EID-2133	Node selection error.	There is an error selecting the node.
EID-2134	File not found. Unable to store overhead circuit preferences.	File not found. Unable to store overhead circuit preferences.
EID-2135	I/O error. Unable to store overhead circuit preferences.	Input/Output error. Unable to store overhead circuit preferences.
EID-2136	Circuit rename failed. {0}	CTC could not rename the circuit.
EID-2137	Merge circuits error.	There was an error merging the circuits.
EID-2138	Cannot delete all destinations. Please try again.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2139	Error updating destinations.	There was an error updating the circuit destinations.
EID-2140	Merge circuits error.	There was an error merging the circuits.
EID-2141	No circuits selected. {0}	You did not select a circuit.
EID-2142	Circuit deletion error.	There was an error deleting the circuit.
EID-2143	No online help version selected. Cannot delete the online help book.	You cannot delete the online help.
EID-2144	Error deleting online help book(s). {0}	You cannot delete the online help.
EID-2145	Unable to locate a node with an IOS card.	Unable to locate a node with a Cisco IOS card.
EID-2146	Security violation. You may only logout your own account.	Refer to error message text.
EID-2147	Security violation. You may only change your own account.	Refer to error message text.
EID-2148	Security violation. You may not delete the account under which are currently logged in.	Refer to error message text.
EID-2173	Port unavailable. The desired CTC CORBA (IIOP) listener port, {0}, is already in use or you do not have permission to listen on it. Please select an alternate port.	The port is unavailable. The desired CTC Common Object Request Broker Architecture (CORBA) Internet Inter-ORB Protocol (IIOP) listener port is already in use or you do not have permission to listen on it. Please select an alternate port.
EID-2174	Invalid number entered. Please check it and try again.	You entered an invalid firewall port number.
EID-2175	Extension byte mismatch. {0}	There is a mismatch with the extension byte.
EID-2176	Not all spans have the same OSPF Area ID. This will cause problems with protection switching. To determine the OSPF Area for a given span, place the cursor mouse over the span and the OSPF Area will be displayed.	Refer to error message text.
EID-2177	Extension byte mismatch. {0}	There is a mismatch with the extension byte.
EID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to error message text.
EID-2179	There is no update as the circuit has been deleted.	Because the circuit has been deleted, there is no update for it.
EID-2180	CTC initialization failed in step {0}.	CTC initialization failed in the specified step.
EID-2181	This link may not be included as it originates from the destination.	Refer to error message text.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2184	Cannot enable the Spanning Tree Protocol (STP) on some ports because they have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign ethernet ports VLANs	Refer to error message text.
EID-2185	Cannot assign the VLANs on some ports because they are incompatible with the STP. You can view the VLAN/Spanning Tree table or reassign VLANs	Refer to error message text.
EID-2186	Software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The maximum length for the ring name that can be used is {0}. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID within the specified range.
EID-2189	TL1 keyword "all" can not be used as the ring name. Please provide another name.	Refer to error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	Refer to error message text.
EID-2191	Ring name must not be empty	You must supply a ring name.
EID-2192	Cannot find a valid route for the circuit creation request.	Refer to error message text.
EID-2193	Cannot find a valid route for the circuit drop creation request.	Refer to error message text.
EID-2194	Cannot find a valid route for the roll creation request.	Refer to error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2196	Unable to relaunch the CTC. {0}	There is an error relaunching CTC.
EID-2197	CORBA failure. Unable to proceed.	There was a CORBA failure, and the task cannot proceed.
EID-2198	Unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified task.
EID-2200	CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one.	Refer to error message text.
EID-2201	{0}	CTC encountered an error.
EID-2202	Intra-node circuit must have 2 sources to be Dual Ring Interconnect.	Intra-node circuit must have two sources to be a dual-ring interconnect (DRI).
EID-2203	No member selected.	You must select a member.
EID-2204	Number of circuits must be a positive integer	The number of circuits cannot be negative.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2205	Circuit Type must be selected	You must select a circuit type.
EID-2206	Unable to autoselect profile! Please select profile(s) to store and try again.	Refer to error message text.
EID-2207	You cannot add this span. Either the ring name is too big (i.e., ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	You cannot add this span. Either the ring name is too big (that is, the ring name length is greater than the specified length) or the endpoints do not support alphanumeric IDs.
EID-2208	This is an invalid or unsupported JRE	The version of Java Runtime Environment (JRE) is either invalid or unsupported.
EID-2209	The user name must be at least {0} characters long.	The user name must be at least the specified character length.
EID-2210	No package name selected	You must select a package name.
EID-2211	No node selected for upgrade	You must select a node for the upgrade.
EID-2212	Protected Line is not provisionable	The protected line cannot be provisioned.
EID-2214	The node is disconnected. Please wait till the node reconnects.	Refer to error message text.
EID-2215	Error while leaving {0} page.	There was an error while leaving the specified page.
EID-2216	Error while entering {0} page.	There was an error entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to error message text.
EID-2218	Bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	Protection operation failed, XC loopback is applied on cross-connection	Protection operation failed; a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is INCOMPLETE. CTC will not be able to change it. Please try again later	Refer to error message text.
EID-2990	Ethernet circuits must be bidirectional.	You attempted to make an Ethernet circuit unidirectional.
EID-2991	Error while creating connection object at {0}.	There was an error creating a connection object at the specified location.
EID-2992	DWDM Link can be used only for Optical Channel circuits.	The dense wavelength division multiplexing (DWDM) link can be used only for optical channel network connection (OCHNC) circuits.
EID-2993	Ochnc circuit link excluded - wrong direction.	The OCHNC circuit link is excluded because it is in the wrong direction.
EID-2994	DWDM Link does not have Wavelength available.	Refer to error message text.
EID-2995	Laser already ON.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	An Ethernet remote monitoring (RMON) threshold with the same parameters already exists. Please change one or more of the parameters and try again.
EID-3002	Error retrieving defaults from the node {0}	There was an error retrieving the defaults from the specified node.
EID-3003	Cannot load file {0}	CTC cannot load the specified file.
EID-3004	Cannot load properties from the node	Refer to error message text.
EID-3005	Cannot save NE Update values to file {0}	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	Cannot load NE Update properties from the node	Refer to error message text.
EID-3007	Provisioning Error for {0}	There was a provisioning error for the specified item.
EID-3008	Not a Barolo Card	You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Shelf view and try again.
EID-3009	No {0} selected	No item selected.
EID-3010	Unable to Create Bidirectional Optical Link	Refer to error message text.
EID-3011	The file {0} doesn't exist or cannot be read	The specified file does not exist or cannot be read.
EID-3012	The size of {0} is zero	The size of the item is zero.
EID-3013	{0} encountered while restoring DB	The specified item was encountered while restoring the database (DB).
EID-3014	Job terminated, {0} was encountered	The job terminated because the specified item was encountered.
EID-3015	{0} encountered while performing DB backup	The specified item was encountered while performing the DB backup.
EID-3016	Invalid subnet address	Refer to error message text.
EID-3017	Subnet address already exists	Refer to error message text.
EID-3018	Standby TSC not ready	The standby Timing and Shelf Control card (TSC) not ready.
EID-3019	Incomplete internal subnet address	There is an incomplete internal subnet address.
EID-3020	TSC One and TSC Two subnet addresses cannot be the same	Refer to error message text.
EID-3021	{0}	CTC encountered an error.
EID-3022	Requested action not allowed	The requested action is not allowed.
EID-3023	Unable to retrieve Low Order Cross Connect Mode	Refer to error message text.
EID-3024	unable to switch Low Order Cross Connect Mode	Refer to error message text.
EID-3025	Error in getting thresholds	The was an error retrieving the thresholds.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3026	Cannot modify Send DoNotUse	CTC cannot modify Send DoNotUse.
EID-3027	Cannot modify EnableSyncMsg	CTC cannot modify EnableSyncMsg.
EID-3028	Cannot change port type	CTC cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port	Refer to error message text.
EID-3031	Error hard-resetting card	There was an error hard-resetting card.
EID-3032	Error resetting card	There was an error resetting the card.
EID-3033	The lamp test is not supported on this shelf	Refer to error message text.
EID-3034	Communication failure	There was a communication failure.
EID-3035	The Cross Connect Diagnostics cannot be performed	Refer to error message text.
EID-3036	The Cross Connect Diagnostics test is not supported on this shelf/CORBA.BAD_OPERATION	The cross-connect diagnostics test is not supported on this shelf.
EID-3037	A software downgrade cannot be performed to the selected version while a SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	A software downgrade cannot be performed to the selected version while a Single-Shelf Cross-Connect (SSXC) card is inserted in this shelf. Please follow the steps to replace the SSXC with a Core Cross-Connect card (CXC) card before continuing the software downgrade.
EID-3038	A software downgrade cannot be performed at the present time.	Refer to error message text.
EID-3039	Card change error	There was a card change error.
EID-3040	Invalid card type	The card type is invalid.
EID-3041	Error Applying Changes	There was an error applying the changes.
EID-3042	The Flow Ctrl Lo value must be less than the Flow Ctrl Hi value for all ports in the card.	Refer to error message text.
EID-3043	Error in getting Line Info settings	Refer to error message text.
EID-3044	Error in getting Line Admin Info settings	Refer to error message text.
EID-3045	Error in getting Transponder Line Admin Info settings	Refer to error message text.
EID-3046	The flow control water mark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the specified values.
EID-3047	The file named {0} could not be read. Please check the name and try again.	The specified file could not be read. Please check the name and try again.
EID-3048	There is no IOS startup config file available to download.	There is no Cisco IOS startup configuration file available to download.
EID-3049	There was a software error attempting to download the file. Please try again later.	Refer to error message text.
EID-3050	An exception was caught trying to save the file to your local file system	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3051	The maximum size for a config file in bytes is {0}	The maximum size for a configuration file in bytes is the value specified in the message.
EID-3052	There was an error saving the config file to the TCC.	Refer to error message text.
EID-3053	The value of {0} must be between {1} and {2}	The value of the item must be between the specified values.
EID-3054	Cannot remove provisioned input/output ports or another user is updating the card, please try later.	Cannot remove provisioned input/output ports or another user is updating the card. Please try later.
EID-3055	Can't Create Soak Maintance Pane	CTC cannot create Soak Maintenance Pane.
EID-3056	Cannot save defaults to file {0}	Cannot save defaults to the specified file.
EID-3057	Cannot load default properties from the node	Refer to error message text.
EID-3058	File {0} does not exist	The specified file does not exist.
EID-3059	Error in refreshing	There was an error in refreshing.
EID-3060	The ALS Recovery Interval must be between 100 seconds and 300 seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between 100 seconds and 300 seconds.
EID-3061	The ALS Recovery Pulse Width must be between 2.00 seconds and 100.0 seconds.	The ALS Recovery Pulse Width must be between 2.00 seconds and 100.0 seconds.
EID-3062	Error in setting values	Refer to error message text.
EID-3063	Error in getting Bridge Port settings	Refer to error message text.
EID-3064	Not a G1000 Card	This card is not a G1000 card.
EID-3065	Create Ether Threshold	You must create an Ethernet threshold.
EID-3066	Minimum sample period must be greater than or equal to 10	Refer to error message text.
EID-3067	Rising Threshold Invalid Entry, valid range is from 1 to {0}	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	Falling Threshold Invalid Entry, valid range is from 1 to {0}	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.
EID-3069	Rising Threshold must be greater than or equal to Falling Threshold	Refer to error message text.
EID-3070	Error in Data For Ports {0} Exactly one VLAN must be marked Untagged for each port. These changes will not be applied.	There was an error in the data for the specified ports. Exactly one VLAN must be marked Untagged for each port. These changes will not be applied.
EID-3071	Get Learned Address	Unable to retrieve the learned MAC address from the NE..
EID-3072	Clear Learned Address	Failure attempting to clear the learned MAC address from a specific card or ethergroup.
EID-3073	Clear Selected Rows	Failure attempting to clear the learned MAC address from a specific card or ethergroup.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3074	Clear By {0}	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in Param column needs to be selected.	Refer to error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to error message text.
EID-3077	No Optical Link Selected	Refer to error message text.
EID-3078	Unable to Create Optical Link	Refer to error message text.
EID-3079	Cannot apply defaults to node {0}	Cannot apply defaults to the specified node.
EID-3080	Cannot go to the target tab {0}	Cannot go to the target tab.
EID-3081	Port type can't be changed	Refer to error message text.
EID-3082	Cannot modify the {0} extension byte	Cannot modify the extension byte.
EID-3083	Error in getting stats	Error in getting statistics.
EID-3084	OSC termination is in use. Error deleting OSC Termination	Optical service channel (OSC) termination is in use. Error deleting OSC termination.
EID-3085	No OSC Terminations selected	Refer to error message text.
EID-3086	One or more Osc terminations could not be created	Refer to error message text.
EID-3087	OSC termination could not be edited	Refer to error message text.
EID-3088	No {0} card to switch	No card of the specified type to switch.
EID-3089	Can't use/change {0} state when {0} is failed or missing.	Cannot use/change the specified state when it is failed or missing.
EID-3090	Can't perform operation as {0} is {1}LOCKED_ON/LOCKED_OUT.	Cannot perform operation.
EID-3091	Can't perform the operation as protect is active.	Refer to error message text.
EID-3092	Can't perform the operation in module's current state.	Refer to error message text.
EID-3093	Can't perform the operation as duplex pair is {0}locked.	Refer to error message text.
EID-3094	Can't perform the operation as no XC redundancy is available.	Refer to error message text.
EID-3095	Deletion failed since the circuit is in use	Refer to error message text.
EID-3096	The Ring ID could not be created	Refer to error message text.
EID-3097	The ring termination is in use.	Refer to error message text.
EID-3098	No Ring Terminations selected	Refer to error message text.
EID-3099	Sorry, entered key does not match existing Authentication key.	The entered key does not match existing authentication key.
EID-3100	Error in authentication	There was an error in authentication.
EID-3101	DCC Metric is not in the range 1 - 65535.	The DCC Metric is not in the range 1 to 65535.
EID-3102	Invalid DCC Metric	There was an Invalid DCC Metric.
EID-3103	Invalid IP Address {0}	The IP Address is Invalid.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3104	Router priority is not in the range of 0 - 255	The Router priority is not in the range of 0 to 255.
EID-3105	Invalid Router Priority	The Router Priority is Invalid.
EID-3106	Hello Interval is not in the range of 1 - 65535	The Hello Interval is not in the range of 1 to 65535.
EID-3107	Invalid Hello Interval	The Hello Interval is Invalid.
EID-3108	Dead Interval is not in the range 1 - 0x7fffffff	The Dead Interval is not in the range 1 to 0x7fffffff.
EID-3109	Invalid Dead Interval	The Dead Interval is invalid.
EID-3110	Dead Interval must be larger than Hello Interval	Refer to error message text.
EID-3111	LAN transit delay is not in the range of 1 - 3600 seconds	The LAN transit delay is not in the range of 1 to 3600 seconds.
EID-3112	Invalid Transit Delay	The transmit delay is invalid.
EID-3113	Retransmit Interval is not in the range 1 - 3600 seconds	The retransmit interval is not in the range 1 to 3600 seconds.
EID-3114	Invalid Retransit Int	The retransmit interval is invalid.
EID-3115	LAN Metric is not in the range 1 - 65535.	The LAN Metric is not in the range 1 to 65535.
EID-3116	Invalid LAN Metric	The LAN Metric is invalid.
EID-3117	If OSPF is active on LAN, no DCC Area Ids may be 0.0.0.0. Please change all DCC Area Ids to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to error message text.
EID-3118	If OSPF is active on LAN, LAN Area ID may not be the same as DCC Area Id.	Refer to error message text.
EID-3119	Validation Error	There is a validation error.
EID-3120	No object of type {0} selected to delete	No object of the selected type selected to delete.
EID-3121	Error Deleting {0}	There is an error deleting the item.
EID-3122	No object of type {0} selected to edit	No object of the specified type selected to edit.
EID-3123	Error Editing {0}	There was an error editing the item.
EID-3124	{0} termination is in use. Check if {0} is used by IPCC.	The specified termination is in use.
EID-3125	No {0} Terminations selected	No specified terminations are selected.
EID-3126	{0} termination could not be edited	The specified termination could not be edited.
EID-3127	Unable to provision orderwire because E2 byte is in use by BLSR.	Refer to error message text.
EID-3128	The authentication key may only be {0} characters maximum	The authentication key can only be the specified characters maximum.
EID-3129	The authentication keys do not match!	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3130	Error creating Area Virtual Link	CTC encountered an error creating the Area Virtual Link.
EID-3131	Error creating Virtual Link	CTC encountered an error creating the Virtual Link.
EID-3132	Error setting area range {0}, {1}, false.	CTC encountered an error setting the area range for the specified values.
EID-3133	Max number Of Area Ranges Exceeded	The maximum number of area ranges has been exceeded.
EID-3134	Invalid Area ID. Use DCC OSPF Area ID, LAN Port Area ID, or 0.0.0.0.	Refer to error message text.
EID-3135	Invalid Mask	Refer to error message text.
EID-3136	Invalid Range Address	Refer to error message text.
EID-3137	Your request has been rejected because the timing source information was updated while your changes were still pending. Please retry.	Refer to error message text.
EID-3138	Invalid clock source for switching.	Refer to error message text.
EID-3139	Cannot switch to a reference of inferior quality.	Refer to error message text.
EID-3140	Higher priority switch already active.	Refer to error message text.
EID-3141	Attempt to access a bad reference.	Refer to error message text.
EID-3142	No Switch Active.	Refer to error message text.
EID-3143	Error creating Static Route Entry	Refer to error message text.
EID-3144	Max number Of Static Routes Exceeded	The maximum number of static routes has been exceeded.
EID-3145	RIP Metric is not in the range 1-15.	The Routing Information Protocol (RIP) metric is not in the range 1 to 15.
EID-3146	Invalid RIP Metric	Refer to error message text.
EID-3147	Error creating Summary Address	Refer to error message text.
EID-3148	No Layer 2 domain selected	Refer to error message text.
EID-3149	Unable to retrieve MAC addresses	Refer to error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writeable.	The specified target file is not writeable.
EID-3152	Error creating Protection Group	CTC encountered an error creating Protection Group.
EID-3153	Cannot delete card, it is in use	Cannot delete card. It is in use.
EID-3154	Cannot {0} card, provision error	CTC cannot perform the task on the card.
EID-3155	Error Building Menu	CTC encountered an error building the menu.
EID-3156	Error on building menu (cards not found for {0} group)	CTC encountered an error on building menu (cards not found for the specified group).

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3157	setSelectedModel unexpected model class {0}	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Unable to switch, a similar or higher priority condition exists on peer or far-end card	Refer to error message text.
EID-3159	Error applying operation	CTC encountered an error applying this operation.
EID-3160	{0} Error	CTC encountered the displayed error.
EID-3161	Ring Upgrade Error	Refer to error message text.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to error message text.
EID-3163	Cannot validate data for row {0}	Cannot validate data for the specified row.
EID-3164	New Node ID ({0}) for Ring ID {1} duplicates ID of node {3}	The new specified Node ID for the specified Ring ID is the same as the second specified Node ID.
EID-3165	Ring IDs must be unique	Refer to error message text.
EID-3166	Error refreshing {0} table	CTC encountered an error refreshing the specified table.
EID-3167	Slot already in use	Refer to error message text.
EID-3169	Error Adding Card	CTC encountered an error adding the card.
EID-3170	Cannot delete card, {0}	Cannot delete the specified card.
EID-3171	Error creating Trap Destination	CTC encountered an error creating the trap destination.
EID-3172	No Ether Thresholds selected	Refer to error message text.
EID-3173	The contact '{0}' exceeds the limit of {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The location '{0}' exceeds the limit of {1} characters.	The specified location exceeds the specified character limit.
EID-3175	The operator identifier '{0}'exceeds the limit of {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific info '{0}'exceeds the limit of {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The name '{0}' is empty!	The specified name is empty.
EID-3178	The name '{0}' exceeds the limit of {1} characters.	The specified name exceeds the specified character limit.
EID-3179	Protect card is in use	Refer to error message text.
EID-3180	1+1 Protection Group does not exist.	Refer to error message text.
EID-3181	Y Cable Protection Group does not exist.	Refer to error message text.
EID-3182	The Topology Element is in use and can't be deleted as requested	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3183	Error Deleting Protection Group	CTC encountered an error deleting the protection group.
EID-3184	No {0} selected	You must select an item before completing this task.
EID-3185	There is a protection switch operation on this ring. Therefore, it cannot be deleted at this time.	Refer to error message text.
EID-3186	Busy {0} is {1} and cannot be deleted as requested.	The item is in use and cannot be deleted as requested.
EID-3187	Error deleting Trap Destination	CTC encountered an error deleting the trap destination.
EID-3188	Invalid UCP Node ID value	Invalid Unified Control Plane (UCP) Node ID value.
EID-3189	Invalid Circuit Retry Initial Interval value	Refer to error message text.
EID-3190	Invalid Circuit Retry Max Interval value	Refer to error message text.
EID-3191	Invalid RSVP Recovery value	Invalid Resource Reservation Protocol (RSVP) recovery value.
EID-3192	Invalid RSVP Refresh value	Refer to error message text.
EID-3193	Invalid RESV timeout value	Invalid reservation (RESV) timeout value.
EID-3194	Invalid RESV CONF timeout value	Invalid reservation confirmation (RESV CONF) timeout value.
EID-3195	Invalid Source Deletion in Progress timeout value	Refer to error message text.
EID-3196	Invalid Destination Deletion in Progress timeout value	Refer to error message text.
EID-3197	Unable to delete circuit origin/termination {0}	Unable to delete the specified circuit origin/termination.
EID-3198	Error refreshing UCP circuit table	Refer to error message text.
EID-3199	Unable to delete UCP Interface {0}	Unable to delete the specified UCP interface.
EID-3200	TNA Address may not be empty	Transport network assigned (TNA) address cannot be empty.
EID-3201	Error refreshing UCP Interface table	Refer to error message text.
EID-3202	Unable to delete IPCC {0}	Unable to delete the specified IP contact center (IPCC).
EID-3203	{0} IPCC may not be empty	The specified IPCC cannot be empty.
EID-3204	Invalid {0} IPCC value	The specified IPCC value is invalid.
EID-3205	MTU value may not be empty for SDCC IPCC	The maximum transmission unit (MTU) value can not be empty for SDCC IPCC.
EID-3206	MTU value may not be negative	MTU value cannot be negative.
EID-3207	Error refreshing IPCC table	Refer to error message text.
EID-3208	Unable to delete neighbor {0}	Unable to delete the specified neighbor.
EID-3209	Neighbor name may not be empty.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3210	Neighbor name may not exceed {0} characters	Neighbor name cannot exceed the specified number of characters.
EID-3211	Error refreshing table	Encountered an error while responding to an update event from the NE. Unable to properly refresh the table values.
EID-3212	IPCC Create Error	Error creating the IPCC.
EID-3213	UCP Neighbor Create Error	Error creating the UCP neighbor.
EID-3214	Could not get number of HOs for line	Refer to error message text.
EID-3215	Error in refreshing	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	Invalid Proxy Port	Invalid Proxy port.
EID-3217	Could not refresh stats.	Could not refresh statistics.
EID-3218	Launch ANS	Launch advanced network service (ANS).
EID-3219	Refresh ANS	Failure trying to retrieve optical link information.
EID-3220	Error refreshing row {0}	Error refreshing the specified row.
EID-3221	Communication Error	Refer to error message text.
EID-3222	Could not clear stats	Refer to error message text.
EID-3223	Error cancelling software upgrade	Refer to error message text.
EID-3224	Error accepting load	Refer to error message text.
EID-3225	Error in pane refresh	Refer to error message text.
EID-3226	Error refreshing page	Refer to error message text.
EID-3227	Could not set baseline	Refer to error message text.
EID-3228	Error refreshing screen	Refer to error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	RIP is active on the LAN. Please disable RIP before enabling OSPF.
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	OSPF is active on the LAN. Please disable OSPF before enabling RIP.
EID-3231	Error in Set OPR	Error in setting optical power received (OPR).
EID-3232	Cannot transition port state indirectly: try editing directly	Refer to error message text.
EID-3233	Current loopback provisioning does not allow this state transition	Refer to error message text.
EID-3234	Current synchronization provisioning does not allow this state transition	Refer to error message text.
EID-3235	Cannot transition state on monitored port	Refer to error message text.
EID-3236	DB Restore failed. {0}	The specified database restore failed.
EID-3237	DB Backup failed. {0}	The specified database backup failed.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3238	Send PDIP setting on {0} is inconsistent with that of control node {1}	Send payload defect indication (PDIP) setting on the specified item is inconsistent with that of the specified control node.
EID-3239	The overhead termination is invalid	Refer to error message text.
EID-3240	The maximum number of overhead terminations has been exceeded	Refer to error message text.
EID-3241	The {0} termination port is in use	The specified termination port is in use.
EID-3242	LDCC exists on the selected ports. Please create SDCC one by one.	The line DCC (LDCC) exists on the selected ports. Please create SDCC one by one.
EID-3244	SDCC exists on the selected ports. Please create LDCC one by one.	SDCC exists on the selected ports. Please create LDCC one by one.
EID-3246	{0}	CTC encountered an error.
EID-3247	Ordering error. The absolute value should be {0}	Ordering error. The absolute value should be the number specified.
EID-3248	Wrong parameter is changed: {0}	CTC changed the wrong parameter.
EID-3249	Invalid voltage increment value.	Refer to error message text.
EID-3250	Invalid power monitor range.	Refer to error message text.
EID-3251	Unable to complete requested action. {0}	CTC is unable to complete requested action.
EID-3252	No download has been initiated from this CTC	Refer to error message text.
EID-3253	Reboot operation failed. {0}	The reboot operation failed.
EID-3254	{0}	CTC encountered an error.
EID-3255	Can not change timing configuration, manual/force operation is performed.	Refer to error message text.
EID-3257	Duplicate DCC number detected: {0}.	CTC detected a duplicate DCC number.
EID-3258	There was a software error attempting to download the file. Please try again later.	Refer to error message text.
EID-3259	Create Fcmr Threshold	You must create an FCMR threshold.
EID-3260	Error refreshing page {0}.	There was an error refreshing the specified page.
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	CTC does not allow you to change the port rate from 1-Gbps to 2-Gbps if a VCAT STS-24c circuit exists on the port. Software Release 4.6 only supports line-rate SONET circuits.
EID-3262	The port provisioning cannot be changed when the port status is not OOS.	Refer to error message text.
EID-3264	The port provisioning cannot be changed while the port is in service.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3265	Error modifying Protection Group	There was an error modifying the protection group.
EID-3266	Conditions could not be retrieved from the shelf or card view	Refer to error message text.
EID-3267	Cannot edit XTC protection group	Refer to error message text.
EID-3268	Invalid entry. {0}	The entry is invalid.
EID-3269	{0} was successfully initiated for {1} but its completion status was not able to be obtained from the node. {0} may or may not have succeeded. When the node is accessible, check its software version.	The specified task was successfully initiated for the item, but its completion status was not able to be obtained from the node. The task might or might not have succeeded. When the node is accessible, check its software version.
EID-3270	The file {0} does not exist.	The specified file does not exist.
EID-3271	The value entered must be greater than {0}.	The value entered must be greater than the value shown.
EID-3272	Entry required	An entry is required for this task.
EID-3273	{0} already exists in the list.	The specified item already exists in the list.
EID-3290	The ALS Recovery Pulse Width must be between 80.00 seconds and 100.0 seconds.	Refer to error message text.
EID-3291	Cannot Change Revertive Behavior due to an active protection switch	Refer to error message text.
EID-3938	Unable to Perform Operation.	CTC is unable to perform operation.
EID-3939	Wrong Node Side.	This task was applied to the wrong node side.
EID-3940	Name too long.	The name you entered is too long.
EID-3941	Illegal name.	The name you entered is illegal.
EID-3942	Wrong line selection.	You selected the wrong line.
EID-3945	Unable to Delete Optical Link	CTC is unable to delete the optical link.
EID-3946	No NetworkType Available	There is no network type available.
EID-3947	At Least One Equipment Is Not Plugged	At least one equipment is not plugged in.
EID-3948	Apc System Is Busy	Automatic power control (APC) system is busy.
EID-3949	No Path To Regulate	There is no circuit path to be regulated.
EID-3950	Requested action not allowed.	Generic DWDM provisioning failure message.
EID-3951	Wrong input value.	The input value is incorrect.
EID-3952	Error in getting thresholds.	There was an error retrieving the thresholds.
EID-3953	Error applying changes to row {0}. Value out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3954	Invalid mode for current configuration.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3955	Unable to switch to the byte because.an overhead channel is present on this byte of the port.	Refer to error message text.
EID-3956	Error applying changes to row	There was an error applying changes to the row.
EID-3957	Error on setting expected wavelength	There was an error setting the expected wavelength.
EID-3958	Error on setting expected band	There was an error setting the expected band.
EID-3959	might parameters on Protect Port.	You cannot change timing parameters on protect port.
EID-3960	This port's type cannot be changed SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	This port's type cannot be changed. The SDH validation check failed. Check to see if this port is part of a circuit, protection group, SONET DCC, orderwire, or User Network Interface, client (UNI-C) interface.
EID-3961	getControlMode	The Control Mode must be retrieved.
EID-3962	setGainSetPoint	The Gain Set Point must be set.
EID-3963	getGainSetPoint	The Gain Set Point must be retrieved.
EID-3964	setTiltCalibration	The tilt calibration must be set.
EID-3965	setExpectedWavelength	The expected wavelength must be set.
EID-3966	getExpectedWavelength	The expected wavelength must be retrieved.
EID-3967	getActualWavelength	The actual wavelength must be retrieved.
EID-3968	getActualBand	The actual band must be retrieved.
EID-3969	getExpectedBand	The expected band must be retrieved.
EID-3970	setExpectedBand	The expected band must be set.
EID-3971	Error retrieving defaults from the node {0}.	There was an error retrieving defaults from the specified node.
EID-3972	Cannot load file {0}	CTC cannot load the specified file.
EID-3973	Cannot load properties from the node	CTC cannot load properties from the node.
EID-3974	Cannot save NE Update values to file	CTC cannot save NE Update values to file.
EID-3975	Cannot load NE Update properties from the node	CTC cannot load NE Update properties from the node.
EID-3976	File {0} does not exist.	The specified file does not exist.
EID-3977	Error on setting value at {0}	There was an error setting the value at the specified location.
EID-3978	NoSuchInterface.	No such interface exists in CTC.
EID-3979	EndPointInUse.	The end point is in use.
EID-3980	EndPointIncompatible.	The end point is incompatible.
EID-3981	Unable to call	CTC is unable to call.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3982	Unable to Calculate Connections.	CTC is unable to calculate connections.
EID-3983	OptLinkModel does not exist for index =	The OptLinkModel does not exist for the specified index.
EID-3984	Unable to call ANS.setNodeOpticalParam CannotPerform.	Refer to error message text.
EID-3985	Unable to call ANS.setNodeOpticalParam FeatureUnsupported.	Refer to error message text.
EID-3986	ring termination is in use. Error deleting ring Termination.	Refer to error message text.
EID-3987	Error deleting ring Termination.	There was an error deleting ring termination.
EID-3988	No Ring Terminations selected.	You must select a ring termination.
EID-3989	Error creating Ring ID.	There was an error creating the ring ID.
EID-3990	OSC termination is in use.	The OSC termination is in use.
EID-3991	Error deleting OSC Termination.	There was an error deleting the OSC termination.
EID-3992	No OSC Terminations selected.	There are no OSC terminations selected.
EID-3993	One or more Osc termination could not be created.{0}	The specified OSC termination could not be created.
EID-3994	OSC termination could not be edited.	The OSC termination could not be edited.
EID-3995	No Optical Link selected.	You must select an optical link.
EID-3996	ERROR on calculate automatic optical link list.	There was an error calculating the automatic optical link list.
EID-3997	Attempt to access an Ochnc Connection that has been destroyed.	You attempted to access an OCHNC connection that has been destroyed.
EID-3998	Tunnel Type Could not be changed Do you wish to roll back?	The tunnel type could not be changed. Do you wish to roll back?
EID-3999	Tunnel repair failed	CTC could not repair the tunnel.
EID-9990	Test message with no variable data.	Refer to error message text.
WID-2149	There is nothing exportable on this view.	Refer to error message text.
WID-2150	Node not initialized. Please wait and try again.	Refer to error message text.
WID-2151	Wait until all the circuits have been repaired to begin a bridge and roll operation on the circuits.	Refer to error message text.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to error message text.
WID-2153	Adding this drop makes the circuit a PCA circuit.	Refer to error message text.
WID-2154	Disallow creating monitor circuits on a port grouping circuit.	Refer to error message text.
WID-2155	Only partial switch count support on some nodes. {0}	Refer to error message text.
WID-2156	Manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error free.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
WID-2157	Cannot complete roll(s). {0}	CTC cannot complete the roll(s).
WID-2158	Invalid roll mode. {0}	The selected roll mode is invalid.
WID-2159	Roll not ready for completion. {0}	The roll is not ready for completion.
WID-2160	Roll not connected. {0}	The selected roll is not connected.
WID-2161	Sibling roll not complete. {0}	The sibling roll is not complete.
WID-2162	Error during roll acknowledgement. {0}	There was an error during the roll acknowledgement.
WID-2163	Cannot cancel roll. {0}	CTC cannot cancel the roll.
WID-2164	Roll error. {0}	CTC encountered a roll error.
WID-2165	The MAC address of node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	The MAC address of the specified node has been changed. All circuits originating from or dropping at this node need to be repaired.
WID-2166	Unable to insert node into the domain. The node is not initialized.	Refer to error message text.
WID-2167	Insufficient security privilege to perform this action.	You have insufficient security privilege to perform this action.
WID-2168	Warnings loading {0}. {1}	CTC encountered warnings while loading the specified item.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	Refer to error message text.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add profile {1}.	The profile list on the specified node is full. Please delete one or more profiles if you wish to add the specified profile.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to error message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The specified CTC CORBA (IIOP) listener port setting will be applied on the next CTC restart.
WID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The current type or state of some drops does not allow the specified new circuit state to be applied to them indirectly.
WID-3243	LDCC exists on the selected port. Please remove one after the connection is created.	Refer to error message text.
WID-3245	SDCC exists on the selected port. Please remove one after the connection is created.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
WID-3256	Could not assign timing reference(s) because at least one timing reference has already been used and/or a timing reference has been attempted to be used twice. Please use the "Reset" button and verify the settings.	Refer to error message text.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	You are using the Java version specified in the first sentence of this message. CTC should run with the Java version specified in the second sentence of this message. The correct Java version can be obtained from the installation CD or at http://java.sun.com/j2se/.
WID-3274	A software upgrade is in progress. Network configuration changes that results a node reboot can not take place during software upgrade. Please try again after software upgrade is done.	Refer to error message text.
WID-3275	Make sure the Remote Interface ID and the Local Interface ID on the two sides are matched. (Local Interface ID on this node should equal Remote Interface ID on the neighbor node and vice-versa).	Refer to error message text.
WID-3276	Both SDCC and LDCC exist on the same selected port. {0}	Both SDCC and LDCC exist on the same selected port.
WID-3277	The description can't contain more than {0} characters. Your input will be truncated.	Refer to error message text.
WID-3278	{0} is not initialized. Please wait and try again.	The specified object is not initialized. Please wait and try again.
WID-3279	Card Deleted, Returning to shelf View	This card has been deleted. CTC is returning to shelf view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS	ALS will not engage until both the protected trunk ports detect loss of service (LOS).
WID-3281	A software upgrade is in progress. {0} can not proceed during a software upgrade. Please try again after the software upgrade has completed.	A software upgrade is in progress. The specified operation can not proceed during a software upgrade. Please try again after the software upgrade has completed.
WID-3283	There is a protection switch or another protection operation applied on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to error message text.
WID-3284	Protection Channel Access circuit found on {0} being set to non-revertive. These circuits will not be able to re-establish after ring or span switch. OK to continue?	Refer to error message text.
WID-3285	Applying FORCE or LOCKOUT operations may result in traffic loss.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error ID	Error Message	Description
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to error message text.
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to error message text.
WID-3288	This ring status is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Refer to error message text.
WID-3289	This node is provisioned to have No LAN Access. Deleting the last DCC may lead to loss of communication with the node. Continue?	Refer to error message text.

INDEX

A

AIP
  MEA 2-148
  replace 3-12
air filter, replace 3-5
AIS 2-21
AIS-L 2-22
AIS-P 2-22
  DS-3 card does not report 1-91
AIS-V 1-89, 2-23
alarms
  alarms are indexed individually by name
  alphabetical list 2-6
  list of critical alarms 2-2
  list of major alarms 2-2
  list of minor alarms 2-3
  TL1 2-1
alarms by description
  improper APS 2-27
alarm troubleshooting 2-1 to 2-220
ALS 2-23
AMI coding 2-121, 2-122
AMPLI-INIT 2-24
APC-DISABLED 2-24
APC-FAIL 2-25
APSB 2-26
APSCDFLTK 2-27
APSC-IMP 2-27, 2-28
APSCINCON 2-29
APSCM 2-29
APSCNMIS 2-30, 2-31
APSMM 2-32
ARP 1-85
AS-CMD 2-32
AS-MT 2-33
asynchronous mapping 2-168
AUD-LOG-LOSS 2-34
AUD-LOG-LOW 2-34
AUTOLSROFF 2-35
automatic protection switching
  byte failure 2-26
  channel failure on protect card 2-93
  channel mismatch 2-30
  invalid K bytes 2-27
  invalid k bytes 2-28
  mode mismatch failure 2-32
  path protection alarms 2-37, 2-38
  path protection revertive switch occurred 2-39
  path protection switch (condition) 2-36, 2-38
  ring switch failure 2-79
  span switch failure 2-81
automatic reset 2-36
AUTORESET 2-36
AUTOSW-AIS 2-36
AUTOSW-LOP (STSMON) 2-37
AUTOSW-LOP (VT-MON) 2-37
AUTOSW-PDI 2-38
AUTOSW-SDBER 2-38
AUTOSW-SFBER 2-38
AUTOSW-UNEQ (STSMON) 2-39
AUTOSW-UNEQ (VTMON) 2-39
AWG-DEG 2-40
AWG-FAIL 2-40
AWG-OVERTEMP 2-41
AWG-WARM-UP 2-41

B

B8ZS 2-120, 2-122

BER

SF-L condition 2-182

verify threshold level 2-219

bit error rate *see* BER

BITS

daisy-chained 1-93

errors 1-92

holdover timing 1-93

loss of frame 2-120

loss of signal 2-127

BKUPMEMP 2-42

BLSR

exercise ring failure 2-76

far-end protection line failure 2-93

improper configuration (alarms) 2-27

lockout condition 2-118

manual ring switch condition 2-177

manual span condition 2-147

ring mismatch 2-176

ring switch failure 2-80

squelch alarm 2-186

BLSROSYNC 2-43

BNC connector 2-173, 2-202

browser

applet security restrictions 1-77

does launch Java 1-68

stalls during download 1-74

C

cache, redirect Netscape cache 1-75

cards

replace 2-219

reseat 2-219

CARLOSS

cause of TPTFAIL 2-200

CARLOSS (EQPT) 2-44

CARLOSS (E-Series) 2-45

CARLOSS (G-Series) 2-46

CARLOSS (ML-Series) 2-49

carrier loss 2-44, 2-45, 2-46, 2-49

CASETEMP-DEG 2-50

CBIT framing 1-36

circuits

AIS-V alarm on DS3XM-6 card 1-89

circuit state transition error 1-88

delete 2-217

effect of a node name change 1-62

identify circuit state 1-89

identify failure points 1-6, 1-8, 1-37

troubleshooting 1-6, 1-8

VT1.5 creation error 1-90

CKTDOWN 2-51

CLDRESTART 2-53

COMIOXC 2-54

COMM-FAIL 2-54

conditions are indexed individually by name

CONTBUS-A-18 2-55

CONTBUS-B-18 2-55

CONTBUS-IO-A 2-56

CONTBUS-IO-B 2-57

cross-connect cards

main payload bus failure 2-61

switching matrix failure 2-193

test standby 1-13, 1-17, 1-27, 1-30, 1-45

CTC

applet not loaded 1-68

applet security restrictions 1-77

delete cache files 1-75

grey node icon 1-77

list of alarms 2-1

log-in errors 1-68, 1-74, 1-81

login errors 1-77

loss of TCP/IP connection 2-44

release interoperability problems 1-80

username and password mismatch 1-81

verifying PC connection 1-70, 1-71

CTNEQPT-PBPROT 2-58, 2-59

CTNEQPT-PBWORK 2-61

cyclic redundancy checking (CRC) 2-42

D

database

parameters that are not restored 1-62

database memory exceeded 2-62

DATAFLT 2-62

DBOSYNC 2-62

DCC

connection loss 1-82

create or verify DCC terminations 2-214

delete a DCC termination 2-107

limitations with OC-3 1-92

default K alarm 2-27

DS3-MISM 2-64

DS3XM-6 card

AIS-V alarm and unused VT circuits 1-89

FEAC features 1-35

incomplete circuit from DS-3 card 1-91

DS-N cards

facility loopback example 1-2

failure to switch 2-78

frame format mismatch 2-64

identify points of failure on circuit path 1-6, 1-8

idle DS-3 signal 2-90

line alarms 2-211

LOF 2-121, 2-122

loopback facility alarm 2-141

loopback signal received 2-139

loss of signal 2-128, 2-129

terminal loopback alarm 2-144

test 1-10, 1-24

DSP-COMM-FAIL 2-63

DSP-FAIL 2-63, 2-65

E

east/ west mismatch alarm 2-73

EC1-12 card

terminal loopback condition 2-144

EC-N card

loopback facility alarm 2-141

LOS 2-130

EHIBATVG-A 2-66, 2-100, 2-145

EIAs

facility loopback test 1-2, 1-9, 1-22

replace 3-17

test 1-11, 1-24

electrical cabling 1-10, 1-23

ELWBATVG-A 2-66

EOC 2-66, 2-68

EQPT 2-69

EQPT-MISS 2-70

equipment failure

far-end DS-1 failure 2-85

far-end DS-3 failure 2-87, 2-88

hardware failure on reporting card 2-69

missing fan-tray assembly 2-70

ERFI-P-CONN 2-71

ERFI-P-PAYLD 2-71

ERFI-P-SRVR 2-71

ERROR-CONFIG 2-72, 2-73

Ethernet

carrier loss 2-45, 2-46

configuring VLANs 1-86

connectivity problems 1-83

Tag/Untag port connectivity 1-85

troubleshooting connections 1-83

E-W-MISMATCH 2-73

EXCCOL 2-75

excess collisions 2-75

EXERCISE-RING-FAIL 2-76

exercise ring failure 2-76

EXERCISE-SPAN-FAIL 2-76

EXT 2-77

external switching commands

- clear a path protection span lock out 2-215
- initiate a 1+1 lock out 3-3
- initiate a path protection Force switch 3-3
- lock out a BLSR span 2-215
- side switch a cross-connect card 1-14, 1-17, 1-18, 1-27, 1-28, 1-30, 1-31, 1-46, 2-216
- switch 1+1 traffic 2-216

EXTRA-TRAF-PREEMPT 2-77

F

facility loopback

- definition 1-2
- G1000-4 port 1-38
- intermediate node G1000-4 1-47
- intermediate node OC-N 1-47
- OC-N port 1-38
- source DS-N port 1-9, 1-22
- test a source DS-N port 1-7, 1-8, 1-22
- test the circuit 1-9, 1-23, 1-39

FAILTOSW 2-78

FAILTOSW-PATH 2-79

FAILTOSWR 2-79

FAILTOSWS 2-81

FAN 2-83

FANDEGRADE 2-84

fan-tray assembly

- MEA 2-151
- missing unit alarm 2-70
- reseat 2-220

FEAC 1-35

FE-AIS 2-84

FEC-MISM 2-84

FE-DS1-MULTLOS 2-85

FE-DS1-NSA 2-85

FE-DS1-SA 2-86

FE-DS1-SNGLLOS 2-86

FE-DS3-NSA 2-87

FE-DS3-SA 2-88

FE-EQPT-NSA 2-88

FE-FRCDWKSWPR-RING 2-89

FE-FRCDWKSWPR-SPAN 2-89

FE-IDLE 2-90

FE-LOF 2-91

FE-LOS 2-91

FE-MANWKSWPR-RING 2-92

FE-MANWKSWPR-SPAN 2-92

FEPRLF 2-93

fiber and cabling errors 1-94

fiber-optic connections 1-95

FIBERTEMP-DEG 2-94

flash manager 2-42

flow rate 2-75

FORCED-REQ 2-94

FORCED-REQ-RING 2-94

FORCED-REQ-SPAN 2-95

FRCDSWTOINT 2-95

FRCDSWTOPRI 2-95

FRCDSWTOSEC 2-96

FRCDSWTOTHIRD 2-96

free run synchronization 2-96

FRNGSYNC 1-93, 2-96

FSTSYNC 2-97

FULLPASSTHR-BI 2-97

G

G1000-4 card

- alarms 2-200
- CARLOSS alarm 2-46
- LPBKFACILITY 2-142
- LPBKTERMINAL 2-143, 2-144
- test 1-39, 1-50, 1-56

GAIN-HDEG 2-97

GAIN-HFAIL 2-98

GAIN-LDEG 2-98

GAIN-LFAIL 2-99
GBIC 1-98
GBICs
  replace 3-18
GCC-EOC 2-100

H

hairpin circuit
  create on source node port 1-12, 1-26
  definition 1-6, 1-7
  perform on source node port 1-12, 1-25
  test hairpin loopback 1-13, 1-26
hardware replacement compatibility 3-9
HI-LASERBIAS 2-101
HI-RXPOWER 2-102
HITEMP 2-103
HI-TXPOWER 2-103
HLDOVRSYNC 1-92, 2-104

I

idle signal condition 2-90
I-HITEMP 2-105
improper APS code. *See* APSC-IMP
improper card removal 2-106
IMPROPRMVL 2-105
INC-ISD 2-109
INCOMPATIBLE-SW 1-80
INHSWPR 2-110
INHSWWKG 2-110
Internet Explorer 1-61
interoperability 1-80
INTRUSION-PSWD 2-111
INVMACADR 2-111
IOSCFGCOPY 2-113
IP
  connectivity 1-81
  designing subnets 1-83

J

Java
  browser does not launch 1-68
  Jave Runtime Environment 1-78
JRE
  description 1-79
  incompatibility 1-78
  launch failure 1-68

K

KB-PASSTHR 2-114
K bytes 2-27
k bytes 2-27, 2-28, 2-114

L

lamp test 1-104
LAN (CAT-5) cable 1-97
LASER-APR 2-115
LASERBIAS-DEG 2-115
LASERBIAS-FAIL 2-116
LASEREOL 2-116
LASERTEMP-DEG 2-117
LED
  blinking STAT LED 1-93
  test 1-104
line coding 2-104, 2-120
line framing 2-120, 2-121
line interface unit 1-2
LKOUTPR-S 2-118
LMP-HELLODOWN 2-118
LMP-NDFAIL 2-118
LOC 2-119
lock out

see also external switching commands
clear a BLSR lock out 2-215
clear a USPR lock out 2-215
lock out a 1+1 3-3
lock out a BLSR 2-215
LOCKOUT-REQ 2-119
LOF (BITS) 2-120
LOF (DS-1) 2-121
LOF (DS3) 2-122
LOF (EC-N) 2-123
LOF (OC-N) 2-121, 2-123, 2-124
log-in errors
browser login does not launch Java 1-68
browser stallls when downloading .jar file 1-74
login errors
applet security restrictions 1-77
no DCC connection 1-82
no IP connectivity 1-81
username/password mismatch 1-81
LOM 2-124
loopback
alarms 2-139, 2-140, 2-142, 2-143, 2-144
clear 2-217
description 1-2
see also facility loopback
see also terminal loopback
LOP-P 2-125
LOP-V 2-125
LO-RXPOWER 2-126, 2-137
LOS (BITS) 2-127
LOS (DS-1) 2-128
LOS (DS-3) 2-129
LOS (EC-N) 2-130
LOS (OC-N) 2-132
LOS (TRUNK) 2-135
loss of frame *see* LOF
loss of pointer *see* LOP
loss of signal *see* FE-LOS
Lower backplane cover 3-19
LPBKCRS 2-138
LPBKDS1FEAC 2-139
LPBKDS1FEAC-CMD 2-139
LPBKDS3FEAC 2-139
LPBKDS3FEAC-CMD 2-140
LPBKFACILITY (DS-1 or DS-3) 2-141
LPBKFACILITY (EC-N) 2-141
LPBKFACILITY (G-Series) 2-142
LPBKFACILITY (OC-N) 2-140, 2-142
LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N) 2-144
LPBKTERMINAL (G-Series) 2-143, 2-144

M

MAC address
data memory failure 2-152
invalid 2-111
mismatch 1-85
MAN-REQ 2-145
MANRESET 2-146
MANSWTOINT 2-146
MANSWTOPRI 2-146
MANSWTOSEC 2-146
MANSWTOTHIRD 2-147
MANUAL-REQ-RING 2-147
MANUAL-REQ-SPAN 2-147
MEA (AIP) 2-148
MEA (EQPT) 2-148
MEA (FAN) 2-150
MEM-GONE 2-151
MEM-LOW 2-151
MFGMEM (AIP, BP, Fan-Tray Assembly) 2-151
multiplexer and demultiplexer cards
OPWR-HDEG alarm 2-158
OPWR-LDEG alarm 2-160
OPWR-LFAIL alarm 2-161

N

Netscape Navigator
- clear cache 1-75
- log in 1-61

network testing
- *see* hairpin circuits
- *see* loopbacks

NIC card 1-69, 1-85

NO-CONFIG 2-152

node ID
- change 2-214
- identify 2-213

NOT-AUTHENTICATED 2-153

NOT-AUTHENTICATED (alarm) 1-81

O

OC-N card
- test 1-39

OC-N cards
- *see also specific card names*
- bit errors 1-94
- lockout request condition 2-120
- loopback caveat 1-2
- OC-3 and DCC limitations 1-92
- test 1-50, 1-56
- transmit and receive levels 1-102

ODUK-AIS-PM 2-154

ODUK-BDI-PM 2-154

ODUK-LCK-PM 2-155

ODUK-OCI-PM 2-155

ODUK-SD-PM 2-156

ODUK-SF-PM 2-156

ODUK-TIM-PM 2-156

optical add/drop multiplexer cards
- OPWR-LFAIL alarm 2-161

optical amplifier cards
- OPWR-HDEG alarm 2-158
- OPWR-LDEG alarm 2-160
- OPWR-LFAIL alarm 2-161

optical service channel cards
- OPWR-HDEG 2-158
- OPWR-LDEG 2-160
- OPWR-LFAIL alarm 2-161

OPTNTWMIS 2-157

OPWR-HDEG 2-158

OPWR-HFAIL 2-160

OPWR-LDEG 2-160

OPWR-LFAIL 2-161

OTUK-AIS 2-161

OTUK-BDI 2-162

OTUK-LOF 2-162

OTUK-SD 2-163

OTUK-SF 2-163

P

password/ username mismatch 1-81

path protection
- AIS alarm 2-36
- clear a lockout 2-215
- exercise ring failure 2-76
- failed switch path 2-79
- LOP alarm 2-37
- PDI alarm 2-38
- SD alarm 2-38
- signal failure alarm 2-39

PDI-P 2-164

PEER-NORESPONSE 2-166

ping 1-70, 2-185

PLM-P 2-167

PLM-V 2-167

PORT-CODE-MISM 2-168

PORT-COMM-FAIL 2-168

PORT-MISMATCH 2-169

PORT-MISSING 2-169

power

consumption 1-104
isolate power supply problems 1-103
supply 1-103
power alarms
output power high degrade 2-158
output power low degrade 2-160
PRC-DUPID 2-170
protection group
delete 2-106
perform a traffic switch 2-216
PROTNA 2-170
PTIM 2-171
PWR-REDUN 2-172

R

RAI 2-172
RCVR-MISS 2-173
receive levels 1-102
retrieve IP address 1-71
RFI-L 2-174
RFI-P 2-174
RFI-V 2-175
ring ID
change 2-213
identify 2-213
RING-MISMATCH 2-176
RING-SW-EAST 2-177
RING-SW-WEST 2-177
RSVP-HELLODOWN 2-177
RUNCFG-SAVENEED 2-178

S

SD 2-178
SD-L 2-180
SD-P 2-180
severities, alarm 2-20
SF 2-181, 2-182
SF-L 2-182
SF-P 2-183
SFP 1-98
SFPs
replace 3-19
SFTWDOWN 2-183
SH-INS-LOSS-VAR-DEG-HIGH 2-183
SH-INS-LOSS-VAR-DEG-LOW 2-184
SHUTTER-OPEN 2-184
side switch *see* external switching commands
signal failure 2-39, 2-182
SMB connector 2-173, 2-202
SNTP-HOST 2-185
SPAN-SW-EAST 2-185
SPAN-SW-WEST 2-186
SQUELCH 2-186, 2-187
SSM
failure 2-189
quality level degrade 2-188
synchronization traceability alarm 2-191
timing switch 1-92
SSM-DUS 2-188
SSM-FAIL 2-189
SSM-LNC 2-189
SSM-OFF 2-189
SSM-PRC 2-190
SSM-PRS 2-190
SSM-RES 2-190
SSM-SMC 2-191
SSM-ST2 2-191
SSM-ST3 2-192
SSM-ST3E 2-192
SSM-ST4 2-192
SSM-STU 2-191
SSM-TNC 2-192
STSMON 2-37, 2-39
switching
see automatic protection switching

see external switching commands

SWMTXMOD 2-193

SWTOPRI 2-194

SWTOSEC 2-194

SWTOTHIRD 2-194

SYNC-FREQ 2-195

synchronization status messaging *see* SSM

SYNCPRI 2-195

SYNCSEC 2-196

SYNCTHIRD 2-197

SYSBOOT 2-197

T

TCC+/TCC2 card

flash memory exceeded 2-62

jar file dowload problem 1-74

loss of signal from BITS 2-127

memory capacity exceeded 2-151

TCC+ card

low memory 2-151

reset 2-217

TCC2 card

communication failure (TCC2 card to traffic card) 2-56, 2-57

communication failure (TCC2 to TCC2) 2-55, 2-56

low memory 2-151

reset 2-217

TCP/IP 1-70, 2-44

Telcordia

signal degrade definition 2-178, 2-179, 2-181

signal failure definition 2-182

temperature

fan-tray assembly alarm 2-83

high-temperature alarm 2-103

OC-192 alarm 2-35

terminal loopback

definition 1-3

destination DS-N port 1-18, 1-20, 1-32, 1-34

destination OC-N 1-57

intermediate G1000-4 1-50

intermediate OC-N 1-50

source node G1000-4 port 1-40

source node OC-N port 1-40

source OC-N 1-41

testing

see lamp test

see loopback

see power

TIM 2-198

timing alarms

loss of primary reference 2-196

loss of tertiary reference 2-197

synchronization 2-96, 2-104

timing reference failure 2-97

timing reference

automatic switch to secondary source (condition) 2-194

automatic switch to third timing source (condition) 2-194

change 2-107

manual switch to internal source (condition) 2-146

manual switch to primary source (condition) 2-146

manual switch to second source (condition) 2-146

manual switch to third source (condition) 2-147

switch error 1-92

TL1 alarms 2-1

TPTFAIL (G-Series) 2-200

TPTFAIL (ML-Series) 2-201

transmission failure 2-202

transmit levels 1-102

TRMT 2-201

TRMT-MISS 2-202

troubleshooting 1-1 to 1-106

see also alarm troubleshooting

see also loopback

conditions 2-20

network tests 1-2

severities 2-20

trouble notifications 2-19

U

UNC-WORD 2-203
UNEQ
AUTOSW-UNEQ (STSMON) 2-39
UNEQ-P 2-204
UNEQ-V 2-206
username/password mismatch 1-81

V

VirusScan 1-74
VOA-HDEG 2-207
VOA-HFAIL 2-208
VOA-LDEG 2-208
VOA-LFAIL 2-209
voltage
see battery
VT1.5 creation error 1-90
VTMON 2-39

W

west⁄ east misconnection alarm 2-73
WKSWPR 2-209
WTR 2-210
WTR (condition) 1-61
WVL-MISMATCH 2-210

X

XC loopback 1-44