



## **Cisco ONS 15454 Troubleshooting Guide**

Product and Documentation Release 3.3  
Last Updated: January 10, 2005

### **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-7814323  
Text Part Number: 78-14323-01



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

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

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

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

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

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

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

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

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

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

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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

*Book Title*

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



## About this Manual **xvii**

- Obtaining Documentation **xvii**
  - World Wide Web **xvii**
  - Documentation CD-ROM **xvii**
  - Ordering Documentation **xviii**
  - Documentation Feedback **xviii**
- Obtaining Technical Assistance **xviii**
  - Cisco.com **xviii**
  - Technical Assistance Center **xix**
    - Cisco TAC Web Site **xix**
    - Cisco TAC Escalation Center **xix**

---

## CHAPTER 1

## Alarm Troubleshooting **1-1**

- 1.1 Alarm Index **1-1**
- 1.2 Alarm Index by Alarm Type **1-3**
  - 1.2.1 Alarm Type/Object Definition **1-8**
- 1.3 Trouble Notifications **1-9**
  - 1.3.1 Conditions **1-9**
  - 1.3.2 Severities **1-9**
- 1.4 Safety Summary **1-10**
- 1.5 Alarm Procedures **1-11**
  - 1.5.1 AIS **1-11**
    - Clear the AIS Condition **1-11**
  - 1.5.2 AIS-L **1-11**
    - Clear the AIS-L Condition **1-11**
  - 1.5.3 AIS-P **1-12**
    - Clear the AIS-P Condition **1-12**
  - 1.5.4 AIS-V **1-12**
    - Clear the AIS-V Condition **1-13**
  - 1.5.5 APSB **1-13**
    - Clear the APSB Alarm **1-13**
  - 1.5.6 APSCDFLTK **1-13**
    - Clear the APSCDFLTK Alarm **1-13**
  - 1.5.7 APSC-IMP **1-14**

- Clear the APSC-IMP Alarm **1-14**
- 1.5.8 APSCINCON **1-15**
  - Clear the APSCINCON Alarm **1-15**
- 1.5.9 APSCM **1-15**
  - Clear the APSCM Alarm **1-16**
- 1.5.10 APSCNMIS **1-16**
  - Clear the APSCNMIS Alarm **1-16**
- 1.5.11 APSMM **1-17**
  - Clear the APSMM Alarm **1-17**
- 1.5.12 AUTOLSROFF **1-18**
  - Clear the AUTOLSROFF Alarm **1-18**
- 1.5.13 AUTORESET **1-18**
  - Clear the AUTORESET Alarm **1-19**
- 1.5.14 AUTOSW-AIS **1-19**
- 1.5.15 AUTOSW-LOP (STSMON) **1-19**
- 1.5.16 AUTOSW-LOP (VT-MON) **1-19**
- 1.5.17 AUTOSW-PDI **1-20**
- 1.5.18 AUTOSW-SDBER **1-20**
- 1.5.19 AUTOSW-SFBER **1-20**
- 1.5.20 AUTOSW-UNEQ (STSMON) **1-20**
- 1.5.21 AUTOSW-UNEQ (VT-MON) **1-20**
- 1.5.22 BKUPMEMP **1-20**
  - Clear the BKUPMEMP Alarm **1-21**
- 1.5.23 BLSROSYNC **1-22**
  - Clear the BLSROSYNC Alarm **1-22**
- 1.5.24 CARLOSS (E-Series) **1-23**
  - Clear the CARLOSS Alarm **1-23**
- 1.5.25 CARLOSS (EQPT) **1-25**
  - Clear the CARLOSS Alarm **1-25**
- 1.5.26 CARLOSS (G1000-4) **1-26**
  - Clear the CARLOSS Alarm **1-26**
- 1.5.27 CLDRESTART **1-28**
  - Clear the CLDRESTART Condition **1-29**
- 1.5.28 CONCAT **1-29**
  - Clear the CONCAT Alarm **1-29**
- 1.5.29 CONTBUS-A **1-30**
  - Clear the CONTBUS-A Alarm **1-30**
- 1.5.30 CONTBUS-A-18 **1-31**
  - Clear the CONTBUS-A-18 Alarm **1-31**
- 1.5.31 CONTBUS-B **1-31**

- Clear the CONTBUS-B [1-32](#)
- 1.5.32 CONTBUS-B-18 [1-33](#)
  - Clear the CONTBUS-B-18 Alarm [1-33](#)
- 1.5.33 CTNEQPT-PBPROT [1-33](#)
  - Clear the CTNEQPT-PBPROT Alarm [1-34](#)
- 1.5.34 CTNEQPT-PBWORK [1-35](#)
  - Clear the CTNEQPT-PBWORK Alarm [1-35](#)
- 1.5.35 DATAFLT [1-36](#)
- 1.5.36 DS3-MISM [1-37](#)
  - Clear the DS3-MISM [1-37](#)
- 1.5.37 EHIBATVG-A [1-37](#)
- 1.5.38 EHIBATVG-B [1-38](#)
- 1.5.39 ELWBATVG-A [1-38](#)
- 1.5.40 ELWBATVG-B [1-38](#)
- 1.5.41 EOC [1-38](#)
  - Clear the EOC Alarm [1-39](#)
- 1.5.42 EQPT [1-40](#)
  - Clear the EQPT Alarm [1-40](#)
- 1.5.43 EQPT-MISS [1-41](#)
  - Clear the EQPT-MISS Alarm [1-41](#)
- 1.5.44 E-W-MISMATCH [1-41](#)
  - Clear the E-W-MISMATCH Alarm with a Physical Switch [1-42](#)
  - Clear the E-W-MISMATCH Alarm [1-42](#)
- 1.5.45 EXCCOL [1-43](#)
  - Clear the EXCCOL Alarm [1-43](#)
- 1.5.46 EXERCISE-RING-FAIL [1-43](#)
  - Clear the EXERCISE-RING-FAIL Condition [1-43](#)
- 1.5.47 EXERCISE-SPAN-FAIL [1-44](#)
  - Clear the EXERCISE-SPAN-FAIL Condition [1-44](#)
- 1.5.48 EXT [1-44](#)
  - Clear the EXT Alarm [1-44](#)
- 1.5.49 FAILTOSW [1-44](#)
  - Clear the FAILTOSW Condition [1-45](#)
- 1.5.50 FAILTOSW-PATH [1-45](#)
  - Clear the FAILTOSW-PATH on a UPSR Configuration [1-45](#)
- 1.5.51 FAILTOSWR [1-47](#)
  - Clear the FAILTOSWR on a Four-Fiber BLSR Configuration [1-47](#)
- 1.5.52 FAILTOSWS [1-48](#)
- 1.5.53 FAN [1-48](#)
  - Clear the FAN Alarm [1-49](#)

1.5.54	FE-AIS	1-49	
	Clear the FE-AIS Condition	1-49	
1.5.55	FE-DS1-MULTLOS	1-50	
	Clear the FE-DS1-MULTLOS Condition	1-50	
1.5.56	FE-DS1-SNGLLOS	1-50	
	Clear the FE-DS1-SNGLLOS Condition	1-50	
1.5.57	FE-DS3-SA	1-50	
	Clear the FE-DS3-SA Condition	1-51	
1.5.58	FE-EQPT-NSA	1-51	
	Clear the FE-EQPT-NSA Condition	1-51	
1.5.59	FE-IDLE	1-51	
	Clear the FE-IDLE Condition	1-52	
1.5.60	FE-LOCKOUT	1-52	
	Clear the FE-LOCKOUT Condition on a BLSR	1-52	
1.5.61	FE-LOF	1-52	
	Clear the FE-LOF Condition	1-52	
1.5.62	FE-LOS	1-53	
	Clear the FE-LOS Condition	1-53	
1.5.63	FEPRLF	1-53	
	Clear the FEPRLF Alarm on a Four-Fiber BLSR	1-53	
1.5.64	FORCED-REQ	1-53	
	Clear the FORCED-REQ	1-54	
1.5.65	FRNGSYNC	1-54	
	Clear the FRNGSYNC Alarm	1-54	
1.5.66	FSTSYNC	1-54	
1.5.67	HITEMP	1-54	
	Clear the HITEMP Alarm	1-55	
1.5.68	HLDOVERSYNC	1-55	
	Clear the HLDOVERSYNC Alarm	1-55	
1.5.69	IMPROPRMVL	1-55	
	Clear the IMPROPRMVL Alarm	1-56	
1.5.70	INCOMPATIBLE-SW	1-57	
	Clear the INCOMPATIBLE-SW Alarm	1-57	
1.5.71	INVMACADDR	1-58	
	Clear the INVMACADDR Alarm	1-58	
1.5.72	KB-PASSTHR	1-58	
	Clear the KB-PASSTHR Condition	1-58	
1.5.73	LOCKOUT-REQ	1-58	
	Clear the Lockout Switch Request and the LOCKOUT-REQ Condition	1-58	
1.5.74	LOF (BITS)	1-59	

Clear the LOF Alarm	<b>1-59</b>
1.5.75 LOF (DS1)	<b>1-60</b>
Clear the LOF Alarm	<b>1-60</b>
1.5.76 LOF (DS3)	<b>1-60</b>
Clear the LOF Alarm	<b>1-61</b>
1.5.77 LOF (EC1-12)	<b>1-61</b>
Clear the LOF Alarm	<b>1-61</b>
1.5.78 LOF (OC-N)	<b>1-62</b>
Clear the LOF Alarm	<b>1-62</b>
1.5.79 LOGBUFR90	<b>1-62</b>
Clear the LOGBUFR90 Alarm	<b>1-63</b>
1.5.80 LOGBUFROVFL	<b>1-63</b>
Clear the LOGBUFROVFL Alarm	<b>1-63</b>
1.5.81 LOP-P	<b>1-63</b>
Clear the LOP-P Alarm	<b>1-64</b>
1.5.82 LOP-V	<b>1-65</b>
Clear the LOP-V Alarm	<b>1-65</b>
1.5.83 LOS (BITS)	<b>1-66</b>
Clear the LOS Alarm	<b>1-66</b>
1.5.84 LOS (DS-N)	<b>1-66</b>
Clear the LOS Alarm	<b>1-67</b>
1.5.85 LOS (EC1-12)	<b>1-67</b>
Clear the LOS Alarm	<b>1-67</b>
1.5.86 LOS (OC-N)	<b>1-68</b>
Clear the LOS Alarm	<b>1-68</b>
1.5.87 LPBKDS1FEAC	<b>1-69</b>
1.5.88 LPBKDS3FEAC	<b>1-69</b>
1.5.89 LPBKFACILITY (DS-N or EC1-12)	<b>1-70</b>
Clear the LBKFACILITY Condition	<b>1-70</b>
1.5.90 LPBKFACILITY (OC-N)	<b>1-71</b>
Clear the LBKFACILITY Condition	<b>1-71</b>
1.5.91 LPBKTERMINAL (DS-N, EC1-12)	<b>1-71</b>
Clear the LBKTERMINAL Condition	<b>1-72</b>
1.5.92 LPBKTERMINAL(G1000-4)	<b>1-72</b>
Clear the LPBKTERMINAL Condition	<b>1-72</b>
1.5.93 LPBKTERMINAL (OC-N)	<b>1-72</b>
Clear the LBKTERMINAL Condition	<b>1-73</b>
1.5.94 MAN-REQ	<b>1-73</b>
Clear the Manual Switch and the MAN-REQ Condition	<b>1-73</b>
1.5.95 MANRESET	<b>1-73</b>

1.5.96	MEA (AIP)	<b>1-74</b>
	Clear the MEA Alarm	<b>1-74</b>
1.5.97	MEA (EQPT)	<b>1-74</b>
	Clear the MEA Alarm	<b>1-74</b>
1.5.98	MEA (FAN)	<b>1-76</b>
	Clear the MEA Alarm	<b>1-76</b>
1.5.99	MEM-GONE	<b>1-76</b>
1.5.100	MEM-LOW	<b>1-77</b>
1.5.101	MFGMEM	<b>1-77</b>
	Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane	<b>1-77</b>
1.5.102	NOT-AUTHENTICATED	<b>1-78</b>
	Clear the NOT-AUTHENTICATED Alarm	<b>1-79</b>
1.5.103	PDI-P	<b>1-79</b>
	Clear the PDI-P Condition	<b>1-80</b>
1.5.104	PEER-NORESPONSE	<b>1-81</b>
	Clear the PEER-NORESPONSE Alarm Reported	<b>1-81</b>
1.5.105	PLM-P	<b>1-81</b>
	Clear the PLM-P Alarm	<b>1-82</b>
1.5.106	PLM-V	<b>1-82</b>
	Clear the PLM-V Alarm	<b>1-83</b>
1.5.107	PRC-DUPID	<b>1-83</b>
	Clear the PRC-DUPID Alarm	<b>1-83</b>
1.5.108	PWR-A	<b>1-83</b>
	Clear the PWR-A Alarm	<b>1-84</b>
1.5.109	PWR-B	<b>1-84</b>
	Clear the PWR-B Alarm	<b>1-84</b>
1.5.110	RAI	<b>1-84</b>
	Clear the RAI Condition	<b>1-84</b>
1.5.111	RCVR-MISS	<b>1-85</b>
	Clear the RCVR-MISS Alarm	<b>1-85</b>
1.5.112	RDI-P	<b>1-85</b>
1.5.113	RFI-L	<b>1-85</b>
	Clear the RFI-L Condition	<b>1-85</b>
1.5.114	RFI-P	<b>1-86</b>
	Clear the RFI-P Condition	<b>1-86</b>
1.5.115	RFI-V	<b>1-86</b>
	Clear the RFI-V Condition	<b>1-87</b>
1.5.116	RING-MISMATCH	<b>1-87</b>
	Clear the RING-MISMATCH Alarm	<b>1-87</b>
1.5.117	SD-L	<b>1-87</b>



Clear the SD-L Condition	<b>1-88</b>
1.5.118 SD-P	<b>1-89</b>
Clear the SD-P Condition	<b>1-89</b>
1.5.119 SF-L	<b>1-90</b>
Clear the SF-L Condition	<b>1-91</b>
1.5.120 SF-P	<b>1-92</b>
Clear the SF-P Condition	<b>1-92</b>
1.5.121 SFTWDOWN	<b>1-93</b>
1.5.122 SFTWDOWN-FAIL	<b>1-93</b>
Clear the SFTWDOWN-FAIL Alarm	<b>1-93</b>
1.5.123 SNTP-HOST	<b>1-94</b>
Clear the SNTP-HOST Alarm	<b>1-95</b>
1.5.124 SQUELCH	<b>1-95</b>
Clear the SQUELCH Condition	<b>1-96</b>
1.5.125 SSM-FAIL	<b>1-96</b>
Clear the SSM-FAIL Alarm	<b>1-96</b>
1.5.126 SSM-STU	<b>1-96</b>
Clear the STU Condition	<b>1-97</b>
1.5.127 SWMTXMOD	<b>1-97</b>
Clear the SWMTXMOD Alarm	<b>1-97</b>
1.5.128 SWTOPRI	<b>1-99</b>
1.5.129 SWTOSEC	<b>1-99</b>
1.5.130 SWTOTHIRD	<b>1-99</b>
1.5.131 SYNCPRI	<b>1-99</b>
Clear the SYNCPRI Condition	<b>1-99</b>
1.5.132 SYNCSEC	<b>1-100</b>
Clear the SYNCSEC Alarm	<b>1-100</b>
1.5.133 SYNCTHIRD	<b>1-100</b>
Clear the SYNCTHIRD Alarm	<b>1-100</b>
1.5.134 SYSBOOT	<b>1-101</b>
1.5.135 TIM-P	<b>1-101</b>
Clear the TIM-P Alarm	<b>1-102</b>
1.5.136 TPTFAIL	<b>1-102</b>
Clear the TPTFAIL Alarm	<b>1-102</b>
1.5.137 TRMT	<b>1-103</b>
Clear the TRMT Alarm	<b>1-103</b>
1.5.138 TRMT-MISS	<b>1-103</b>
Clear the TRMT-MISS Alarm	<b>1-103</b>
1.5.139 UNEQ-P	<b>1-104</b>
Clear the UNEQ-P Alarm	<b>1-104</b>

- 1.5.140 UNEQ-V [1-105](#)
  - Clear the UNEQ-V Alarm [1-106](#)
- 1.6 DS3-12E Line Alarms [1-107](#)

**CHAPTER 2**

**General Troubleshooting [2-1](#)**

- 2.1 Network Troubleshooting Tests [2-1](#)
- 2.2 Identify Points of Failure on a Circuit Path [2-3](#)
  - 2.2.1 Perform a Facility Loopback on a Source DS-N Card [2-4](#)
    - 2.2.1.1 Create the Facility Loopback on the Source DS-N Card [2-4](#)
    - 2.2.1.2 Test the Facility Loopback Circuit [2-5](#)
    - 2.2.1.3 Test the DS-N Cabling [2-5](#)
    - 2.2.1.4 Test the DS-N Card [2-5](#)
    - 2.2.1.5 Test the EIA [2-6](#)
  - 2.2.2 Perform a Hairpin on a Source Node [2-7](#)
    - 2.2.2.1 Create the Hairpin on the Source Node [2-7](#)
    - 2.2.2.2 Test the Hairpin Circuit [2-8](#)
    - 2.2.2.3 Test the Standby Cross-Connect Card [2-8](#)
    - 2.2.2.4 Retest the Original Cross-Connect Card [2-9](#)
  - 2.2.3 Perform a Terminal Loopback on a Destination DS-N Card [2-9](#)
    - 2.2.3.1 Create the Terminal Loopback on a Destination DS-N Card [2-10](#)
    - 2.2.3.2 Test the Terminal Loopback Circuit on the Destination DS-N Card [2-11](#)
    - 2.2.3.3 Test the Destination DS-N Card [2-11](#)
  - 2.2.4 Perform a Facility Loopback on a Destination DS-N Card [2-11](#)
    - 2.2.4.1 Create a Facility Loopback Circuit on a Destination DS-N Card [2-12](#)
    - 2.2.4.2 Test the Facility Loopback Circuit [2-12](#)
    - 2.2.4.3 Test the DS-N Cabling [2-13](#)
    - 2.2.4.4 Test the DS-N Card [2-13](#)
    - 2.2.4.5 Test the EIA [2-14](#)
  - 2.2.5 Using the DS3XM-6 Card FEAC (Loopback) Functions [2-14](#)
    - 2.2.5.1 FEAC Send Code [2-15](#)
    - 2.2.5.2 FEAC Inhibit Loopback [2-16](#)
    - 2.2.5.3 FEAC Alarms [2-16](#)
- 2.3 CTC Operation and Connectivity [2-16](#)
  - 2.3.1 Operation: Unable to Change Node View to Network View [2-16](#)
    - 2.3.1.1 Reset the CTC\_HEAP Environment Variable for Windows [2-17](#)
    - 2.3.1.2 Reset the CTC\_HEAP Environment Variable for Solaris [2-17](#)
  - 2.3.2 Operation: Browser Stalls When Downloading CTC JAR Files From TCC+ [2-17](#)
    - 2.3.2.1 Disable the VirusScan Download Scan [2-18](#)
  - 2.3.3 Operation: CTC Does Not Launch [2-18](#)

- 2.3.3.1 Redirect the Netscape Cache to a Valid Directory [2-18](#)
- 2.3.4 Operation: Sluggish CTC Operation or Login Problems [2-19](#)
  - 2.3.4.1 Delete the CTC Cache File Automatically [2-19](#)
  - 2.3.4.2 Delete the CTC Cache File Manually [2-20](#)
- 2.3.5 Operation: Node Icon is Grey on CTC Network View [2-21](#)
- 2.3.6 Operation: CTC Cannot Launch Due to Applet Security Restrictions [2-21](#)
  - 2.3.6.1 Manually Edit the java.policy File [2-21](#)
- 2.3.7 Operation: Java Runtime Environment Incompatible [2-22](#)
  - 2.3.7.1 Launch CTC to Correct the Core Version Build [2-23](#)
- 2.3.8 Operation: Different CTC Releases Do Not Recognize Each Other [2-23](#)
  - 2.3.8.1 Launch CTC to Correct the Core Version Build [2-23](#)
- 2.3.9 Operation: Username or Password Do Not Match [2-24](#)
  - 2.3.9.1 Verify Correct Username and Password [2-24](#)
- 2.3.10 Operation: No IP Connectivity Exists Between Nodes [2-25](#)
- 2.3.11 Operation: DCC Connection Lost [2-25](#)
- 2.3.12 Operation: Browser Login Does Not Launch Java [2-25](#)
  - 2.3.12.1 Reconfigure the PC Operating System and the Browser [2-25](#)
- 2.3.13 Connectivity: Verify PC Connection to ONS 15454 (ping) [2-26](#)
  - 2.3.13.1 Ping the ONS 15454 [2-27](#)
- 2.3.14 Calculate and Design IP Subnets [2-27](#)
- 2.3.15 Ethernet Connections [2-27](#)
  - 2.3.15.1 Verify Ethernet Connections [2-28](#)
- 2.3.16 VLAN Cannot Connect to Network Device from Untag Port [2-29](#)
  - 2.3.16.1 Change VLAN Port Tag and Untagged Settings [2-30](#)
- 2.3.17 Cross-Connect Card Oscillator Fails [2-31](#)
  - 2.3.17.1 Resolve the XC Oscillator Failure When Slot 8 XC Card is Active [2-32](#)
  - 2.3.17.2 Resolve the XC Oscillator Failure When Slot 10 XC Card is Active [2-32](#)
- 2.4 Circuits and Timing [2-33](#)
  - 2.4.1 AIS-V on DS3XM-6 Unused VT Circuits [2-33](#)
    - 2.4.1.1 Clear AIS-V on DS3XM-6 Unused VT Circuits [2-33](#)
  - 2.4.2 Circuit Creation Error with VT1.5 Circuit [2-34](#)
  - 2.4.3 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card [2-34](#)
  - 2.4.4 DS3 Card Does Not Report AIS-P From External Equipment [2-35](#)
  - 2.4.5 OC-3 and DCC Limitations [2-35](#)
  - 2.4.6 ONS 15454 Switches Timing Reference [2-35](#)
  - 2.4.7 Holdover Synchronization Alarm [2-36](#)
  - 2.4.8 Free-Running Synchronization Mode [2-37](#)
  - 2.4.9 Daisy-Chained BITS Not Functioning [2-37](#)
- 2.5 Fiber and Cabling [2-37](#)
  - 2.5.1 Bit Errors Appear for a Traffic Card [2-37](#)

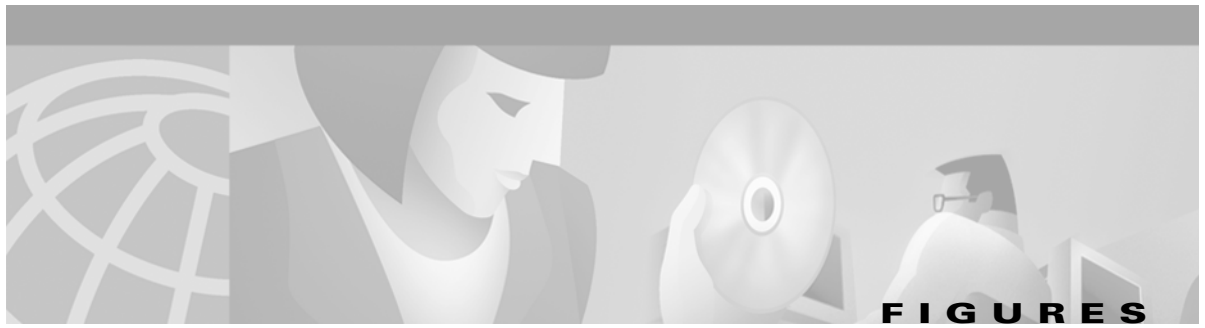
- 2.5.2 Faulty Fiber-Optic Connections **2-38**
  - 2.5.2.1 Verify Fiber-Optic Connections **2-38**
  - 2.5.2.2 Replace Faulty Gigabit Interface Converters **2-40**
  - 2.5.2.3 Crimp Replacement CAT-5 Cables **2-42**
- 2.5.3 Optical Card Transmit and Receive Levels **2-43**
- 2.6 Power and LED Tests **2-44**
  - 2.6.1 Power Supply Problems **2-44**
    - 2.6.1.1 Isolate the Cause of Power Supply Problems **2-45**
  - 2.6.2 Power Consumption for Node and Cards **2-45**
  - 2.6.3 Lamp Test for Card LEDs **2-46**
    - 2.6.3.1 Verify Card LED Operation **2-46**

**CHAPTER 3**

**Replace Hardware 3-1**

- 3.1 Switch Traffic and Replace an In-Service Cross-Connect Card **3-2**
- 3.2 Reset the TCC+ With a Card Pull **3-5**
- 3.3 Replace the Air Filter **3-5**
  - 3.3.1 Inspect, Clean, and Replace the Reusable Air Filter **3-6**
  - 3.3.2 Inspect and Replace the Disposable Air Filter **3-8**
- 3.4 Determine Replacement Hardware Compatibility **3-11**
- 3.5 Replace the Fan-Tray Assembly **3-13**
- 3.6 Replace the Alarm Interface Panel **3-15**
- 3.7 Replace the Electrical Interface Assembly **3-20**

**INDEX**



<i>Figure 2-1</i>	The facility loopback process on a DS-N card	<b>2-2</b>
<i>Figure 2-2</i>	The facility loopback process on an OC-N card	<b>2-2</b>
<i>Figure 2-3</i>	The terminal loopback process on an OC-N card	<b>2-2</b>
<i>Figure 2-4</i>	The terminal loopback process on a DS-N card	<b>2-3</b>
<i>Figure 2-5</i>	The hairpin circuit process on an OC-N card	<b>2-3</b>
<i>Figure 2-6</i>	A facility loopback on a circuit source DS-N card	<b>2-4</b>
<i>Figure 2-7</i>	Hairpin on a source node	<b>2-7</b>
<i>Figure 2-8</i>	Terminal loopback on a destination DS-N card	<b>2-10</b>
<i>Figure 2-9</i>	Facility loopback on a destination DS-N card	<b>2-12</b>
<i>Figure 2-10</i>	Accessing FEAC functions on the DS3XM-6 card	<b>2-15</b>
<i>Figure 2-11</i>	Diagram of far end action code	<b>2-15</b>
<i>Figure 2-12</i>	Deleting the CTC cache	<b>2-20</b>
<i>Figure 2-13</i>	Ethernet connectivity reference	<b>2-28</b>
<i>Figure 2-14</i>	A VLAN with Ethernet ports at Tagged and Untag	<b>2-29</b>
<i>Figure 2-15</i>	Configuring VLAN membership for individual Ethernet ports	<b>2-31</b>
<i>Figure 2-16</i>	A gigabit interface converter (GBIC)	<b>2-40</b>
<i>Figure 2-17</i>	Installing a GBIC on the E1000-2/E1000-2-G card	<b>2-41</b>
<i>Figure 2-18</i>	RJ-45 pin numbers	<b>2-42</b>
<i>Figure 2-19</i>	A straight-through cable layout	<b>2-42</b>
<i>Figure 2-20</i>	A cross-over cable layout	<b>2-43</b>
<i>Figure 3-1</i>	A reusable fan-tray air filter in an external filter bracket (front door removed)	<b>3-7</b>
<i>Figure 3-2</i>	Inserting or removing the fan-tray assembly (front door removed)	<b>3-9</b>
<i>Figure 3-3</i>	Inserting or removing a disposable fan-tray air filter (front door removed)	<b>3-10</b>
<i>Figure 3-4</i>	Removing or replacing the fan-tray assembly (front door removed)	<b>3-14</b>
<i>Figure 3-5</i>	Find the MAC address	<b>3-16</b>
<i>Figure 3-6</i>	Lower backplane cover	<b>3-16</b>
<i>Figure 3-7</i>	Repair Circuits in the Menu Bar	<b>3-18</b>
<i>Figure 3-8</i>	Repairing circuits	<b>3-19</b>
<i>Figure 3-9</i>	Recording the old MAC address before replacing the AIP	<b>3-19</b>
<i>Figure 3-10</i>	Circuit repair information	<b>3-20</b>

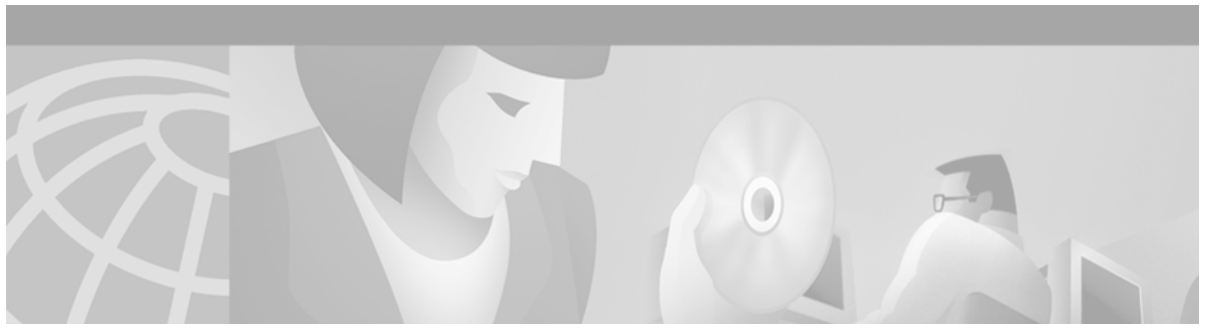




<i>Table 1-1</i>	Alarm Index <a href="#">1-1</a>
<i>Table 1-2</i>	Alarm Index by Alarm Type <a href="#">1-3</a>
<i>Table 1-3</i>	Alarm Type/Object Definition <a href="#">1-8</a>
<i>Table 1-4</i>	DS3-12E Line Alarms <a href="#">1-107</a>
<i>Table 2-1</i>	Browser Stalls When Downloading Files From TCC+ <a href="#">2-16</a>
<i>Table 2-2</i>	Browser Stalls When Downloading jar File From TCC+ <a href="#">2-17</a>
<i>Table 2-3</i>	CTC Does Not Launch <a href="#">2-18</a>
<i>Table 2-4</i>	Sluggish CTC Operation or Login Problems <a href="#">2-19</a>
<i>Table 2-5</i>	Node Icon is Grey on CTC Network View <a href="#">2-21</a>
<i>Table 2-6</i>	CTC Cannot Launch Due to Applet Security Restrictions <a href="#">2-21</a>
<i>Table 2-7</i>	Java Runtime Environment Incompatible <a href="#">2-22</a>
<i>Table 2-8</i>	JRE Compatibility <a href="#">2-22</a>
<i>Table 2-9</i>	Different CTC Releases Do Not Recognize Each Other <a href="#">2-23</a>
<i>Table 2-10</i>	Username or Password Do Not Match <a href="#">2-24</a>
<i>Table 2-11</i>	No IP Connectivity Exists Between Nodes <a href="#">2-25</a>
<i>Table 2-12</i>	DCC Connection Lost <a href="#">2-25</a>
<i>Table 2-13</i>	Browser Login Does Not Launch Java <a href="#">2-25</a>
<i>Table 2-14</i>	Verify PC connection to ONS 15454 (ping) <a href="#">2-26</a>
<i>Table 2-15</i>	Calculate and Design IP Subnets <a href="#">2-27</a>
<i>Table 2-16</i>	Calculate and Design IP Subnets <a href="#">2-27</a>
<i>Table 2-17</i>	Verify PC connection to ONS 15454 (ping) <a href="#">2-30</a>
<i>Table 2-18</i>	Cross-Connect Card Oscillator Fails <a href="#">2-32</a>
<i>Table 2-19</i>	Calculate and Design IP Subnets <a href="#">2-33</a>
<i>Table 2-20</i>	Circuit Creation Error with VT1.5 Circuit <a href="#">2-34</a>
<i>Table 2-21</i>	Unable to Create Circuit from DS-3 Card to DS3XM-6 Card <a href="#">2-35</a>
<i>Table 2-22</i>	DS3 Card Does Not Report AIS-P From External Equipment <a href="#">2-35</a>
<i>Table 2-23</i>	OC-3 and DCC Limitations <a href="#">2-35</a>
<i>Table 2-24</i>	ONS 15454 Switches Timing Reference <a href="#">2-36</a>
<i>Table 2-25</i>	Holdover Synchronization Alarm <a href="#">2-36</a>
<i>Table 2-26</i>	Free-Running Synchronization Mode <a href="#">2-37</a>
<i>Table 2-27</i>	Daisy-Chained BITS Not Functioning <a href="#">2-37</a>

<i>Table 2-28</i>	Bit Errors Appear for a Line Card	<a href="#">2-38</a>
<i>Table 2-29</i>	Faulty Fiber-Optic Connections	<a href="#">2-38</a>
<i>Table 2-30</i>	Straight-through cable pinout	<a href="#">2-42</a>
<i>Table 2-31</i>	Cross-over cable pinout	<a href="#">2-43</a>
<i>Table 2-32</i>	Optical Card Transmit and Receive Levels	<a href="#">2-43</a>
<i>Table 2-33</i>	Power Supply Problems	<a href="#">2-44</a>
<i>Table 2-34</i>	Power Consumption for Node and Cards	<a href="#">2-45</a>
<i>Table 2-35</i>	Lamp Test for Card LEDs	<a href="#">2-46</a>
<i>Table 3-1</i>	Incompatibility Alarms	<a href="#">3-12</a>





## About this Manual

---

The *Cisco ONS 15454 Troubleshooting Guide* provides alarm clearing, general troubleshooting, and hardware replacement procedures.

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

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

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

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

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

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

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

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

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

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

<http://www.cisco.com>

## Technical Assistance Center

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

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

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

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

### Cisco TAC Web Site

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

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

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

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

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

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

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

### Cisco TAC Escalation Center

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

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

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

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



# Alarm Troubleshooting

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

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

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

This chapter provides a comprehensive list of alarms (conditions with a severity of Minor, Major or Critical.) It also includes some conditions with severities of non-alarmed (NA) or not reported (NR), which are commonly encountered while troubleshooting major alarms. The default standby severity for conditions with a severity of NA, Non-service affecting (NSA) is NA, NSA. The default standby severity for conditions with a severity of NR, NSA is NR, NSA. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and ONS 15327 TL1 Command Guide*.

## 1.1 Alarm Index

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

**Table 1-1 Alarm Index**

<a href="#">AIS, page 1-11</a>	<a href="#">EXT, page 1-44</a>	<a href="#">MANRESET, page 1-73</a>
<a href="#">AIS-L, page 1-11</a>	<a href="#">FAILTOSW, page 1-44</a>	<a href="#">MEA (AIP), page 1-74</a>
<a href="#">AIS-P, page 1-12</a>	<a href="#">FAILTOSW-PATH, page 1-45</a>	<a href="#">MEA (EQPT), page 1-74</a>
<a href="#">AIS-V, page 1-12</a>	<a href="#">FAILTOSWR, page 1-47</a>	<a href="#">MEA (FAN), page 1-76</a>
<a href="#">APSB, page 1-13</a>	<a href="#">FAILTOSWS, page 1-48</a>	<a href="#">MEM-GONE, page 1-76</a>
<a href="#">APSCDFLTK, page 1-13</a>	<a href="#">FAN, page 1-48</a>	<a href="#">MEM-LOW, page 1-77</a>
<a href="#">APSC-IMP, page 1-14</a>	<a href="#">FE-AIS, page 1-49</a>	<a href="#">MFGMEM, page 1-77</a>
<a href="#">APSCINCON, page 1-15</a>	<a href="#">FE-DS1-MULTLOS, page 1-50</a>	<a href="#">NOT-AUTHENTICATED, page 1-78</a>
<a href="#">APSCM, page 1-15</a>	<a href="#">FE-DS1-SNGLLOS, page 1-50</a>	<a href="#">PDI-P, page 1-79</a>
<a href="#">APSCNMIS, page 1-16</a>	<a href="#">FE-DS3-SA, page 1-50</a>	<a href="#">PEER-NORESPONSE, page 1-81</a>

Table 1-1 Alarm Index (continued)

APSM, page 1-17	FE-EQPT-NSA, page 1-51	PLM-P, page 1-81
AUTOLSROFF, page 1-18	FE-IDLE, page 1-51	PLM-V, page 1-82
AUTORESET, page 1-18	FE-LOCKOUT, page 1-52	PRC-DUPID, page 1-83
AUTOSW-AIS, page 1-19	FE-LOF, page 1-52	PWR-A, page 1-83
AUTOSW-LOP (STSMON), page 1-19	FE-LOS, page 1-53	PWR-B, page 1-84
AUTOSW-LOP (VT-MON), page 1-19	FEPRLF, page 1-53	RAI, page 1-84
AUTOSW-PDI, page 1-20	FORCED-REQ, page 1-53	RCVR-MISS, page 1-85
AUTOSW-SDBER, page 1-20	FRNGSYNC, page 1-54	RDI-P, page 1-85
AUTOSW-SFBER, page 1-20	FSTSYNC, page 1-54	RFI-L, page 1-85
AUTOSW-UNEQ (STSMON), page 1-20	HITEMP, page 1-54	RFI-P, page 1-86
AUTOSW-UNEQ (VT-MON), page 1-20	HLDOVERSYNC, page 1-55	RFI-V, page 1-86
BKUPMEMP, page 1-20	IMPROPRMVL, page 1-55	RING-MISMATCH, page 1-87
BLSROSYNC, page 1-22	INCOMPATIBLE-SW, page 1-57	SD-L, page 1-87
CARLOSS (E-Series), page 1-23	INVMACADDR, page 1-58	SD-P, page 1-89
CARLOSS (EQPT), page 1-25	KB-PASSTHR, page 1-58	SF-L, page 1-90
CARLOSS (G1000-4), page 1-26	LOCKOUT-REQ, page 1-58	SF-P, page 1-92
CLDRESTART, page 1-28	LOF (BITS), page 1-59	SFTWDOWN, page 1-93
CONCAT, page 1-29	LOF (DS1), page 1-60	SFTWDOWN-FAIL, page 1-93
CONTBUS-A, page 1-30	LOF (DS3), page 1-60	SNTP-HOST, page 1-94
CONTBUS-A-18, page 1-31	LOF (EC1-12), page 1-61	SQUELCH, page 1-95
CONTBUS-B, page 1-31	LOF (OC-N), page 1-62	SSM-FAIL, page 1-96
CONTBUS-B-18, page 1-33	LOGBUFR90, page 1-62	SSM-STU, page 1-96
CTNEQPT-PBPROT, page 1-33	LOGBUFROVFL, page 1-63	SWTOPRI, page 1-99
CTNEQPT-PBWORK, page 1-35	LOP-P, page 1-63	SWTOSEC, page 1-99
DATAFLT, page 1-36	LOP-V, page 1-65	SWTOTHIRD, page 1-99
DS3-MISM, page 1-37	LOS (BITS), page 1-66	SWMTXMOD, page 1-97
EHIBATVG-A, page 1-37	LOS (DS-N), page 1-66	SYNCPRI, page 1-99
EHIBATVG-B, page 1-38	LOS (EC1-12), page 1-67	SYNCSEC, page 1-100
ELWBATVG-A, page 1-38	LOS (OC-N), page 1-68	SYNCTHIRD, page 1-100
ELWBATVG-B, page 1-38	LPBKDS1FEAC, page 1-69	SYSBOOT, page 1-101
EOC, page 1-38	LPBKDS3FEAC, page 1-69	TIM-P, page 1-101
EQPT, page 1-40	LPBKFACILITY (DS-N or EC1-12), page 1-70	TPTFAIL, page 1-102
EQPT-MISS, page 1-41	LPBKFACILITY (OC-N), page 1-71	TRMT, page 1-103
E-W-MISMATCH, page 1-41	LPBKTERMINAL (DS-N, EC1-12), page 1-71	TRMT-MISS, page 1-103
EXCCOL, page 1-43	LPBKTERMINAL(G1000-4), page 1-72	UNEQ-P, page 1-104

Table 1-1 Alarm Index (continued)

EXERCISE-RING-FAIL, page 1-43	LPBKTERMINAL (OC-N), page 1-72	UNEQ-V, page 1-105
EXERCISE-SPAN-FAIL, page 1-44	MAN-REQ, page 1-73	

## 1.2 Alarm Index by Alarm Type

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

Table 1-2 Alarm Index by Alarm Type

AIP::INVMACADDR, page 1-58
AIP::MEA (AIP), page 1-74
AIP::MFGMEM, page 1-77
BITS::AIS, page 1-11
BITS::LOF (BITS), page 1-59
BITS::LOS (BITS), page 1-66
BITS::SSM-FAIL, page 1-96
BPLANE::MFGMEM, page 1-77
DS1::AIS, page 1-11
DS1::LOF (DS1), page 1-60
DS1::LOS (DS-N), page 1-66
DS1::LPBKDS1FEAC, page 1-69
DS1::LPBKFACILITY (DS-N or EC1-12), page 1-70
DS1::LPBKTERMINAL(G1000-4), page 1-72
DS1::RCVR-MISS, page 1-85
DS1::TRMT, page 1-103
DS1::TRMT-MISS, page 1-103
DS3::AIS, page 1-11
DS3::DS3-MISM, page 1-37
DS3::FE-AIS, page 1-49
DS3::FE-DS1-MULTLOS, page 1-50
DS3::FE-DS1-SNGLLOS, page 1-50
DS3::FE-DS3-SA, page 1-50
DS3::FE-EQPT-NSA, page 1-51
DS3::FE-IDLE, page 1-51
DS3::FE-LOF, page 1-52
DS3::FE-LOS, page 1-53
DS3::LOF (DS3), page 1-60

**Table 1-2 Alarm Index by Alarm Type (continued)**

DS3::LOS (DS-N), page 1-66
DS3::LPBKDS1FEAC, page 1-69
DS3::LPBKDS3FEAC, page 1-69
DS3::LPBKFACILITY (DS-N or EC1-12), page 1-70
DS3::LPBKTERMINAL (DS-N, EC1-12), page 1-71
DS3::RAI, page 1-84
E1000F::CARLOSS (E-Series), page 1-23
E100T::CARLOSS (E-Series), page 1-23
EC1-12::AIS-L, page 1-11
EC1-12::LOF (EC1-12), page 1-61
EC1-12::LOS (EC1-12), page 1-67
EC1-12::LPBKFACILITY (DS-N or EC1-12), page 1-70
EC1-12::LPBKTERMINAL (DS-N, EC1-12), page 1-71
EC1-12::RFI-L, page 1-85
ENVARM::EXT, page 1-44
EQPT::AUTORESET, page 1-18
EQPT::BKUPMEMP, page 1-20
EQPT::CARLOSS (EQPT), page 1-25
EQPT::CLDRESTART, page 1-28
EQPT::CONTBUS-A-18, page 1-31
EQPT::CONTBUS-A, page 1-30
EQPT::CONTBUS-B-18, page 1-33
EQPT::CONTBUS-B, page 1-31
EQPT::CTNEQPT-PBPROT, page 1-33
EQPT::CTNEQPT-PBWORK, page 1-35
EQPT::EQPT, page 1-40
EQPT::EXCCOL, page 1-43
EQPT::FAILTOSW, page 1-44
EQPT::FORCED-REQ, page 1-53
EQPT::HITEMP, page 1-54
EQPT::IMPROPRMVL, page 1-55
EQPT::LOCKOUT-REQ, page 1-58
EQPT::MANRESET, page 1-73
EQPT::MEA (EQPT), page 1-74
EQPT::MEM-GONE, page 1-76
EQPT::MEM-LOW, page 1-77
EQPT::PEER-NORESPONSE, page 1-81



**Table 1-2 Alarm Index by Alarm Type (continued)**

EQPT::SWMTXMOD, page 1-97
EQPT::SFTWDOWN, page 1-93
EQPT::SFTWDOWN-FAIL, page 1-93
EXT-SREF::SWTOPRI, page 1-99
EXT-SREF::SWTOSEC, page 1-99
EXT-SREF::SWTOTHIRD, page 1-99
EXT-SREF::SYNCPRI, page 1-99
EXT-SREF::SYNCSEC, page 1-100
EXT-SREF::SYNCTHIRD, page 1-100
FAN::EQPT-MISS, page 1-41
FAN::FAN, page 1-48
FAN::MEA (FAN), page 1-76
FAN::MFGMEM, page 1-77
G1000::CARLOSS (G1000-4), page 1-26
G1000::LPBKTERMINAL(G1000-4), page 1-72
G1000::TPTFAIL, page 1-102
NE::BLSROSYNC, page 1-22
NE::DATAFLT, page 1-36
NE::EHIBATVG-A, page 1-37
NE::EHIBATVG-B, page 1-38
NE::ELWBATVG-A, page 1-38
NE::ELWBATVG-B, page 1-38
NE::HITEMP, page 1-54
NE::KB-PASSTHR, page 1-58
NE::PRC-DUPID, page 1-83
NE::PWR-A, page 1-83
NE::PWR-B, page 1-84
NE::RING-MISMATCH, page 1-87
NE::SNTP-HOST, page 1-94
NE::SYSBOOT, page 1-101
NE-SREF::FRNGSYNC, page 1-54
NE-SREF::FSTSYNC, page 1-54
NE-SREF::HLDOVERSYNC, page 1-55
NE-SREF::SWTOSEC, page 1-99
NE-SREF::SWTOTHIRD, page 1-99
NE-SREF::SYNCPRI, page 1-99
NE-SREF::SYNCSEC, page 1-100

**Table 1-2 Alarm Index by Alarm Type (continued)**

NE-SREF::SYNCTHIRD, page 1-100
OCN::AIS-L, page 1-11
OCN::APSB, page 1-13
OCN::APSCDFLTK, page 1-13
OCN::APSC-IMP, page 1-14
OCN::APSCINCON, page 1-15
OCN::APSCM, page 1-15
OCN::APSCNMIS, page 1-16
OCN::APSM, page 1-17
OCN::AUTOLSROFF, page 1-18
OCN::EOC, page 1-38
OCN::E-W-MISMATCH, page 1-41
OCN::FEPLF, page 1-53
OCN::FORCED-REQ, page 1-53
OCN::LOCKOUT-REQ, page 1-58
OCN::LOF (OC-N), page 1-62
OCN::LOS (OC-N), page 1-68
OCN::LPBKFACILITY (OC-N), page 1-71
OCN::LPBKTERMINAL (OC-N), page 1-72
OCN::SD-L, page 1-87
OCN::SF-L, page 1-90
OCN::SQUELCH, page 1-95
OCN::SSM-FAIL, page 1-96
OCN::SSM-STU, page 1-96
STSMON::AIS-P, page 1-12
STSMON::AUTOSW-AIS, page 1-19
STSMON::AUTOSW-LOP (STSMON), page 1-19
STSMON::AUTOSW-PDI, page 1-20
STSMON::AUTOSW-SDBER, page 1-20
STSMON::AUTOSW-SFBER, page 1-20
STSMON::AUTOSW-UNEQ (STSMON), page 1-20
STSMON::CONCAT, page 1-29
STSMON::FAILTOSW-PATH, page 1-45
STSMON::FORCED-REQ, page 1-53
STSMON::LOCKOUT-REQ, page 1-58
STSMON::LOP-P, page 1-63
STSMON::MAN-REQ, page 1-73

**Table 1-2 Alarm Index by Alarm Type (continued)**

<a href="#">STSMON::PDI-P, page 1-79</a>
<a href="#">STSMON::PLM-P, page 1-81</a>
<a href="#">STSMON::RFI-P, page 1-86</a>
<a href="#">STSMON::TIM-P, page 1-101</a>
<a href="#">STSMON::UNEQ-P, page 1-104</a>
<a href="#">STSRNG::BLSROSYNC, page 1-22</a>
<a href="#">STSRNG::PRC-DUPID, page 1-83</a>
<a href="#">STSRNG::RING-MISMATCH, page 1-87</a>
<a href="#">STSTRM::LOP-P, page 1-63</a>
<a href="#">STSTRM::PLM-P, page 1-81</a>
<a href="#">STSTRM::SD-P, page 1-89</a>
<a href="#">STSTRM::SF-P, page 1-92</a>
<a href="#">STSTRM::TIM-P, page 1-101</a>
<a href="#">STSTRM::UNEQ-P, page 1-104</a>
<a href="#">VT-MON::AIS-V, page 1-12</a>
<a href="#">VT-MON::AUTOSW-AIS, page 1-19</a>
<a href="#">VT-MON::AUTOSW-LOP (VT-MON), page 1-19</a>
<a href="#">VT-MON::AUTOSW-PDI, page 1-20</a>
<a href="#">VT-MON::AUTOSW-SDBER, page 1-20</a>
<a href="#">VT-MON::AUTOSW-SFBER, page 1-20</a>
<a href="#">VT-MON::AUTOSW-UNEQ (VT-MON), page 1-20</a>
<a href="#">VT-MON::FORCED-REQ, page 1-53</a>
<a href="#">VT-MON::LOCKOUT-REQ, page 1-58</a>
<a href="#">VT-MON::LOP-V, page 1-65</a>
<a href="#">VT-MON::UNEQ-V, page 1-105</a>
<a href="#">VT-TERM::AIS-V, page 1-12</a>
<a href="#">VT-TERM::LOP-V, page 1-65</a>
<a href="#">VT-TERM::PLM-V, page 1-82</a>
<a href="#">VT-TERM::RFI-V, page 1-86</a>
<a href="#">VT-TERM::SD-P, page 1-89</a>
<a href="#">VT-TERM::SF-P, page 1-92</a>
<a href="#">VT-TERM::UNEQ-V, page 1-105</a>

## 1.2.1 Alarm Type/Object Definition

*Table 1-3 Alarm Type/Object Definition*

<b>AIP</b>	Auxiliary interface protection module
<b>BITS</b>	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)
<b>BPLANE</b>	The backplane
<b>DS1</b>	A DS1 line on a DS1 or DS3XM card
<b>DS3</b>	A DS3 line on a DS3 or DS3XM card
<b>E1000F</b>	An Ethernet line on an E1000 card
<b>E100T</b>	An Ethernet line on an E100 card
<b>EC1-12</b>	An EC1 line on an EC1 card
<b>ENVALRM</b>	An environmental alarm port on an AIC card
<b>EQPT</b>	A card in any of the 17 card slots. This object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, STS and VT
<b>EXT-SREF</b>	BITS outgoing references (SYNC-BITS1, SYNC-BITS2)
<b>FAN</b>	Fan-tray assembly
<b>G1000</b>	An Ethernet line on a G1000
<b>NE</b>	The entire network element (SYSTEM)
<b>NE-SREF</b>	Represents the timing status of the NE
<b>OCN</b>	An OCN line on an OCN card
<b>STSMON</b>	STS alarm detection at the monitor point (upstream of cross-connect)
<b>STSRNG</b>	BLSR ring number (STSRNG)
<b>STSTRM</b>	STS alarm detection at termination (downstream of cross-connect)
<b>VT-MON</b>	VT1 alarm detection at the monitor point (upstream of cross-connect)
<b>VT-TERM</b>	VT1 alarm detection at termination (downstream of cross-connect)

## 1.3 Trouble Notifications

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

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

### 1.3.1 Conditions

When an SA failure is detected, the ONS 15454 also sends an alarm indication signal (AIS) downstream. When it receives the AIS, the receiving node sends a remote failure indication (RFI) upstream. AIS and RFI belong in the conditions category and show up on the Conditions screen of the ONS 15454. However, unlike most conditions which are non-alarmed, Telcordia classifies these conditions as not reported (NR).

Both CTC and TL1 report NRs and NAs as conditions when conditions are retrieved. NAs are also reported as autonomous events under TL1 and under the History tab of CTC. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

### 1.3.2 Severities

The ONS 15454 uses Telcordia-standard severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service-affecting alarm that needs immediate correction. Major is a serious alarm, but the failure has less of an impact on the network. For example, with a DS1-14 LOS, a Major alarm, 24 DS-0 circuits lose protection. But with a OC-192 LOS, a Critical alarm, over a hundred thousand DS-0 circuits lose protection.

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

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

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

## 1.4 Safety Summary

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



**Caution**

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

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



**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 procedures.



**Warning**

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



**Warning**

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



**Warning**

**Class 1 laser product.**



**Warning**

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

## 1.5 Alarm Procedures

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

### 1.5.1 AIS

- Not Reported (NR)

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

#### Procedure: Clear the AIS Condition

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports. |
| <b>Step 2</b> | Clear the upstream alarms.  |
- 

### 1.5.2 AIS-L

- Not Reported (NR)

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

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

#### Procedure: Clear the AIS-L Condition

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Check upstream nodes and equipment for alarms, especially for LOS and an out-of-service port. |
| <b>Step 2</b> | Clear the upstream alarms.  |
-

## 1.5.3 AIS-P

- Not Reported (NR) (Condition)

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

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

### Procedure: Clear the AIS-P Condition

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Check upstream nodes and equipment for alarms, especially LOS and out-of-service ports. |
| <b>Step 2</b> | Clear the upstream alarms.  |
- 

## 1.5.4 AIS-V

- Not Reported (NR)

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

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

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


**Note**

See the [“AIS-V on DS3XM-6 Unused VT Circuits” section on page 2-33](#) for AIS-Vs that occur on DS3XM-6 unused VT circuits.



## Procedure: Clear the AIS-V Condition

- 
- Step 1** Check upstream nodes and equipment for alarms, especially LOS and out-of-service ports.
- Step 2** Correct the upstream alarms.
- 

## 1.5.5 APSB

- Minor, Non-service affecting

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

## Procedure: Clear the APSB Alarm

- 
- Step 1** Examine the incoming SONET overhead with an optical test set to confirm inconsistent or invalid K bytes.
- Step 2** If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment may not interoperate effectively with the ONS 15454. For ONS 15454 protection switching to operate properly, the upstream equipment may need to be replaced.
- 

## 1.5.6 APSCDFLTK

- Minor, Non-service affecting

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

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

## Procedure: Clear the APSCDFLTK Alarm

- 
- Step 1** Prior to accepting a new mapping table, verify that each node has a unique node ID number.
- a. Log into a node on the ring.
  - b. Click the **Provisioning > Ring** tabs.
  - c. Record the node ID number.
  - d. Repeat these substeps for all nodes in the ring.
-

- e. If two nodes have the same node ID number, change one node's ID number so that each node has a unique node ID.
  - f. Click **Apply**.
- Step 2** Verify correct configuration of east port and west port optical fibers (see the “[E-W-MISMATCH](#)” section on page 1-41).
- Step 3** If it is a four fiber BLSR system, make sure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if there is a working fiber incorrectly attached to a protection fiber.
- Step 4** Click **Yes** to accept the Ring Map.
- Step 5** If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.
- a. At the node (default) view, click the **Provisioning > Ring** tabs.
  - b. Highlight a BLSR.
  - c. Click **Ring Map**.
  - d. Verify that each node that is part of the ring appears on the Ring Map with a Node ID and IP Address.
  - e. Click **Close**.
- Step 6** If nodes are not visible, ensure that SDCC terminations exist on each node.
- a. Click the **Provisioning > SONET DCC** tabs.
  - b. Click **Create**.
  - c. Click the OC-N card that links to the adjacent node.
  - d. Click **OK**.
- Step 7** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

## 1.5.7 APSC-IMP

- Minor, Non-service affecting

An Improper SONET Automatic Protect Switch code alarm indicates invalid K bytes. This alarm occurs on OC-N cards in a BLSR configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. APSCIMP occurs when these bits indicate a bad or invalid K byte. The alarm clears when the node receives valid K bytes.



### Caution

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

### Procedure: Clear the APSC-IMP Alarm

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

- Step 2** If the K byte is invalid, the problem lies in upstream equipment and not in the reporting ONS 15454. Troubleshoot the appropriate upstream equipment.
- Step 3** If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs:
- Using CTC, log into a node on the ring.
  - Click the **Provisioning > Ring** tabs.
  - Record the ring ID number.
  - Repeat these substeps for all nodes in the ring.
- Step 4** If a node has a ring ID number that does not match the other nodes, change the ring ID number of that node to match the other nodes in the ring.
- Step 5** Click **Apply**.
- 

## 1.5.8 APSCINCON

- Minor, Service affecting

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

### Procedure: Clear the APSCINCON Alarm

- Step 1** Look for other alarms, especially LOS, loss of frame (LOF) or AIS. Clearing these alarms clears the APSCINCON alarm.
- Step 2** If an APSINCON alarm occurs with no other alarms, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- 

## 1.5.9 APSCM

- Major, Service affecting

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



#### Warning

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

---

**Warning**

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

**Caution**

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

**Procedure: Clear the APSCM Alarm**

- 
- Step 1** Verify that the working-card channel fibers connect directly to the adjoining node's working-card channel fibers.
- Step 2** Verify that the protection-card channel fibers connect directly to the adjoining node's protection-card channel fibers.
- 

**1.5.10 APSCNMIS**

- Major, Service affecting

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

**Procedure: Clear the APSCNMIS Alarm**

- 
- Step 1** Verify that each node has a unique node ID number.
- Click the **Provisioning > Ring** tabs.
  - Click the BLSR row to highlight.
  - Click **Ring Map**.
  - If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.
  - Click **Close** on the Ring Map dialog box.
- Step 2** If two nodes have the same node ID number, change one node's ID number so that each node has a unique node ID:
- Display the network view.
  - Log into one of the nodes that uses the repeated node ID recorded in [Step 1](#).



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

- c. Click the Node ID table cell to reveal a pull-down menu.
- d. Select a unique node ID from the pull-down menu and click **Apply**.



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

- Step 3** If the alarm does not clear, lock out a span on the ring and then clear the lockout:
- a. Click the **Ring > Maintenance** tabs.
  - b. Click the table cell under the West Switch heading to reveal the pull-down menu.
  - c. Choose **LOCKOUT SPAN** and click **Apply**.
  - d. Click **OK** on the BLSR Operations dialog box.
  - e. Click the same table cell under the West Switch heading to reveal the pull-down menu.
  - f. Choose **CLEAR** and click **Apply**.
  - g. Click **OK** on the BLSR Operations dialog box.

## 1.5.11 APSMM

- Minor, Non-service affecting

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

### Procedure: Clear the APSMM Alarm

- Step 1** For the reporting ONS 15454, display the CTC node view and click the **Provisioning > Protection** tabs.
- Step 2** Choose the 1+1 protection group configured for the OC-N cards.  
This is the protection group optically connected (with DCC connectivity) to the far end.
- Step 3** Record whether the bidirectional switching box is checked.
- Step 4** Log into the far end node and verify that the OC-N 1+1 protection group is provisioned.  
This is the protection group optically connected (with DCC connectivity) to the near end.
- Step 5** Verify that the bidirectional switching box matches the checked or unchecked condition of the box recorded in [Step 3](#). If not, change it to match.

**Step 6** Click **Apply**.

---

## 1.5.12 AUTOLSROFF

- Critical, Service affecting



**Warning**

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

---



**Warning**

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

---

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

### Procedure: Clear the AUTOLSROFF Alarm

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

**Step 2** If the temperature of the ONS 15454 exceeds 90 degrees Centigrade, complete the [“Clear the HITEMP Alarm” procedure on page 1-55](#).

**Step 3** If the temperature of the ONS 15454 is below 90 degrees Centigrade, replace 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. Consult the *Cisco ONS 15454 Procedure Guide* for procedures.

---



**Note**

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

---

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

---

## 1.5.13 AUTORESET

- Minor, Non-service affecting

The AUTORESET alarm occurs when a card performs a warm reboot automatically. This happens when you change an IP address or perform any other operation that causes an automatic card-level reboot.

**Caution**

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

## Procedure: Clear the AUTORESET Alarm

- Step 1** Check for additional alarms that may have triggered an automatic reset.
- Step 2** If the card automatically resets more than once a month with no apparent cause, replace it with a new card.

**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 procedures.

**Note**

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

## 1.5.14 AUTOSW-AIS

- Not Reported (Condition)

AUTOSW-AIS indicates that automatic UPSR protection switching took place because of an AIS alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“AIS” section on page 1-11](#).

## 1.5.15 AUTOSW-LOP (STSMON)

- Not Alarmed (Condition)

AUTOSW-LOP indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“LOP-P” section on page 1-63](#).

## 1.5.16 AUTOSW-LOP (VT-MON)

- Minor, Service affecting

AUTOSW-LOP indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“LOP-P” section on page 1-63](#).

## 1.5.17 AUTOSW-PDI

- Not Alarmed (Condition)

AUTOSW-PDI indicates that automatic UPSR protection switching took place because of a PDI alarm. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“PDI-P” section on page 1-79](#).

## 1.5.18 AUTOSW-SDBER

- Not Alarmed (NA) (Condition)

AUTOSW-SDBER indicates that a signal degrade alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and has switched back to the working path. Troubleshoot with the [“CLDRESTART” section on page 1-28](#).

## 1.5.19 AUTOSW-SFBER

- Not Alarmed (NA) (Condition)

AUTOSW-SFBER indicates that a signal fail alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and will switch back to the working path. Troubleshoot with the [“SF-L” section on page 1-90](#).

## 1.5.20 AUTOSW-UNEQ (STSMON)

- Not Alarmed (Condition)

AUTOSW-UNEQ indicates that a UNEQ alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“UNEQ-P” section on page 1-104](#).

## 1.5.21 AUTOSW-UNEQ (VT-MON)

- Minor, Service affecting

AUTOSW-UNEQ indicates that a UNEQ alarm caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and will switch back to the working path after the fault clears. Troubleshoot with the [“UNEQ-P” section on page 1-104](#).

## 1.5.22 BKUPMEMP

- Critical, Non-service affecting

The BKUPMEMP alarm refers to a problem with the TCC+ card's flash memory. The alarm occurs when the TCC+ card is in use and has one of four problems: the flash manager fails to format a flash partition, the flash manager fails to write a file to a flash partition, there is a problem at the driver level or the code volume fails cyclic redundancy checking (CRC). CRC is a method to check for errors in data transmitted to the TCC+.




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

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

## Procedure: Clear the BKUPMEMP Alarm

- 
- Step 1** Verify that both TCC+ cards are powered and enabled by confirming lighted ACT/STBY LEDs on the TCC+ cards.
- Step 2** If both TCC+ cards are powered and enabled, reset the TCC+ card against which the alarm is raised:
- a. Right-click the TCC+ card in CTC.
  - b. Choose **RESET CARD** from the shortcut menu.
  - c. Click **Yes** in the Are You Sure dialog box.
    - If the card was the active card, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.
    - If the card was the standby card, the FAIL LED blinks on the physical card.
  - d. Wait ten minutes to verify that the card you reset completely reboots.
- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. If the card was the active card, double-click the node and ensure that the reset TCC+ card is in standby mode and that the other TCC+ card is active.
- Step 4** If the TCC+ you reset does not reboot successfully or the alarm has not cleared, reseal the card:
- a. Ensure that the TCC+ you want to reset is in standby mode. On the TCC+ card, the ACT/SBY (Active/Standby) LED is amber when the TCC+ is in standby mode.
  - b. When the TCC+ is in standby mode, unlatch both the top and bottom ejectors on the TCC+ card.
  - c. Physically pull the card at least partly out of the slot until the lighted LEDs turn off.
  - d. Wait 30 seconds. Reinsert the card and close the ejectors.
-  **Note** The TCC+ will take several minutes to reboot and will display the amber standby LED after rebooting.
- 
- Step 5** If the alarm reappears after you perform the switch and reseal the card, replace the TCC+ card.
- a. Open the card ejectors.
  - b. Slide the card out of the slot.
  - c. Open the ejectors on the replacement card.
  - d. Slide the replacement card into the slot along the guide rails.
  - e. Close the ejectors.




---

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

---

## 1.5.23 BLSROSYNC

- Major, Service affecting

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

### Procedure: Clear the BLSROSYNC Alarm

- 
- Step 1** Prior to accepting a new mapping table, verify that each node has a unique node ID number:
- Log into a node on the ring.
  - Click the **Provisioning > Ring** tabs.
  - Record the Node ID number.
  - Repeat these substeps for all nodes in the ring.
  - If two nodes have the same node ID number, change one node ID number, so the node ID number is unique within that ring.
  - Click **Apply**.
- Step 2** Verify that each node has a ring ID that matches the other node ring IDs:
- Log into the next node on the ring.
  - Click the **Provisioning > Ring** tabs.
  - Record the Ring ID number.
  - Repeat these substeps for all nodes in the ring.
  - If a node has a ring ID number that does not match the other nodes, change the ring ID to match all the other nodes in the ring.
  - Click **Apply**.
- Step 3** Verify correct configuration of the east port and west port optical fibers (see the [“E-W-MISMATCH” section on page 1-41.](#))
- Step 4** If it is a four-fiber BLSR system, make sure that each protect fiber connects to another protect fiber, and each working fiber connects to another working fiber. The software does not report any alarm, if there is a working fiber misconnected to a protect fiber.



**Warning**

---

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

---

**Warning**

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

- Step 5** If the east-to-west configuration changes, click **Apply**.  
The BLSR Ring Map Change screen appears.
- Step 6** Click **Yes** to accept the Ring Map.
- Step 7** If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.
- Step 8** If nodes are not visible, ensure that SDCC terminations exist on each node.
- Click the **Provisioning > SONET DCC** tabs.
  - Click **Create**.
  - Click the OC-N card that links to the adjacent node.
  - Click **OK**.
- Step 9** If alarms are raised when the DCCs are turned on, follow the troubleshooting procedure in the “EOC” section on page 1-38.
- Step 10** If the alarm does not clear, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

## 1.5.24 CARLOSS (E-Series)

- Major, Service affecting

A carrier loss on the LAN is the data equivalent of a SONET LOS alarm. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of this alarm are a disconnected cable, an OC-N fiber connected to the Ethernet GBIC or an improperly installed Ethernet card. Ethernet card ports must be enabled (put in service) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

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

**Caution**

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

### Procedure: Clear the CARLOSS Alarm

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

- Step 2** Verify that the Ethernet cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** Check that the transmitting device is operational. If not, troubleshoot the device.
- Step 4** Using a test set, determine that a valid signal is coming into the Ethernet port.
- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the Ethernet cable connecting the transmitting device to the Ethernet port.
- Step 6** If a valid Ethernet signal is present, physically reseat the Ethernet card.
- Step 7** If the alarm does not clear, replace the Ethernet card.

**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 procedures.

---

- a. Open the card ejectors.
- b. Slide the card out of the slot.
- c. Open the ejectors on the replacement card.
- d. Slide the replacement card into the slot along the guide rails.
- e. Close the ejectors.

**Note**


---

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

---

- Step 8** If a CARLOSS alarm repeatedly appears and clears, examine the layout of your particular network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect. If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm may be a result of mismatched STS circuit sizes in the set up of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, these steps do not apply.

**Note**


---

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

---

- a. Right-click anywhere on the row of the CARLOSS alarm.
- b. Right-click or left-click the **Select Affected Circuits** dialog that appears.
- c. Record the information in the type and size columns of the highlighted circuit.
- d. From the examination of the layout of your particular network, determine the ONS 15454 and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.
- e. Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
- f. Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- g. Click the **Circuits** tab.
- h. Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. This circuit will connect the Ethernet card to an OC-N card on the same node.

- i. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
  - j. If one of the circuit sizes is incorrect, navigate to the incorrectly configured circuit.
  - k. Click the incorrectly configured circuit to highlight it and click **Delete**.
  - l. Click **Yes** at the Delete Circuit dialog box, and **OK** at the Confirmation dialog box.
  - m. Reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* to provision Ethernet manual cross-connects.
- 

## 1.5.25 CARLOSS (EQPT)

- Minor, Non-service affecting

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

### Procedure: Clear the CARLOSS Alarm

---

- Step 1** Verify connectivity by pinging the ONS 15454 that is reporting the alarm:
- a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Programs > Command Prompt**.
  - b. If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.

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

```
ping [ONS 15454 IP address]
For example, ping 192.1.0.2.
```

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

- Step 2** If the ping is successful, an active TCP/IP connection exists. Restart CTC.
- Step 3** If you are unable to establish connectivity, perform standard network/LAN diagnostics. For example, trace the IP route, check cables, and check any routers between the node and CTC.
- 

## 1.5.26 CARLOSS (G1000-4)

- Major, Service affecting

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

CARLOSS on the G1000-4 is caused by one of two situations:

a) The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. A common cause is that an Ethernet cable not connected properly to the reporting Ethernet port, an OC-N card is connected to the port instead of an Ethernet device, or there is a problem with the signal from the Ethernet device attached to the G1000-4 port.

b) There is a problem in the end-to-end path (including possibly the remote end G1000-4 card), which is causing the reporting G1000-4 to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-4 port turns the transmitter laser back on, and this clears the CARLOSS on the reporting card. In this case, the CARLOSS alarm will normally be accompanied by another alarm or condition on the end-to-end path, such as a TPTFAIL or an OC-N alarm or condition.

Refer to the *Cisco ONS 15454 Procedure Guide* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the “TPTFAIL” section on page 1-102 for more information on alarms that occur when a point-to-point circuit exists between two G1000-4 cards.

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



### Caution

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

---

## Procedure: Clear the CARLOSS Alarm

- Step 1** Verify that the Ethernet cable is properly connected and attached to the correct port.
- Step 2** Verify that the Ethernet cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** Check that the transmitting attached Ethernet device is operational. If not, troubleshoot the device.

- Step 4** Using an Ethernet test set, determine that a valid signal is coming into the Ethernet port.
- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the Ethernet cable connecting the transmitting device to the Ethernet port.
- Step 6** If link auto negotiation is enabled on the G1000-4 port, but the auto negotiation process fails, the G1000-4 will turn off its transmitter laser and report a CARLOSS alarm. If link auto negotiation has been enabled on the port, check for conditions which could cause auto negotiation to fail:
- Confirm that the attached Ethernet device has auto negotiation enabled and is configured for compatibility with the asymmetric flow control on the G1000-4.
  - Confirm that the attached Ethernet device configuration allows reception of flow control frames.
- Step 7** If all previous attempts fail, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition (this will restart the auto negotiation process).
- Step 8** If the TPTFAIL alarm is also reported, see [“TPTFAIL” section on page 1-102](#). If the TPTFAIL alarm is not reported, continue to the next step.




---

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

---

- Step 9** Check to see if terminal loopback has been provisioned on this port.
- On the G1000-4 card, provisioning a terminal loopback causes the transmit laser to turn off. If an attached Ethernet device detects this as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could cause the CARLOSS alarm detected by the G1000-4 port in loopback.
- a. Click the **Conditions** tab and click **Retrieve Conditions**.
  - b. If LPBKTERMINAL appears in the condition field of the Conditions tab, a terminal loopback has been set on this port.
    - Click **Maintenance > Loopback**.
    - Under the Loopback Type column, select NONE for the port row reporting the alarm.
    - Click **Apply**.
  - c. If LPBKTERMINAL is not in the condition field of the Conditions tab, continue to [Step 10](#).
- Step 10** If a CARLOSS alarm repeatedly appears and clears, examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect. If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm may be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, these steps do not apply.




---

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

---

- a. Right-click anywhere on the row of the CARLOSS alarm.
- b. Right-click or left-click the **Select Affected Circuits** dialog.
- c. Record the information in the type and size columns of the highlighted circuit.

- d. From the examination of the layout of your particular network, determine the ONS 15454 and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.
- e. Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
- f. Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- g. Click the **Circuits** tab.
- h. Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. This circuit will connect the Ethernet card to an OC-N card on the same node.
- i. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
- j. If one of the circuit sizes is incorrect, navigate to the incorrectly configured circuit.
- k. Click the incorrectly configured circuit and click **Delete**.
- l. Click **Yes** at the Delete Circuit dialog box, and **OK** at the Confirmation dialog box.
- m. Reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* to provision Ethernet manual cross-connects.

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

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



**Caution**

---

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

---

- a. Open the card ejectors.
- b. Slide the card out of the slot.
- c. Open the ejectors on the replacement card.
- d. Slide the replacement card into the slot along the guide rails.
- e. Close the ejectors.



**Note**

---

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

---

## 1.5.27 CLDRESTART

- Not Alarmed (NA) (Condition)

A Cold Restart is a cold boot of the reporting card. This alarm can occur when you physically remove and insert a card, power up an ONS 15454, or replace a card.



**Caution**

---

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

---



## Procedure: Clear the CLDRESTART Condition

**Step 1** If the alarm fails to clear after the card reboots, physically reseal the card.

**Step 2** If the alarm fails to clear, replace the card.



**Caution**

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



**Note**

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

## 1.5.28 CONCAT

- Critical, Service affecting

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

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

## Procedure: Clear the CONCAT Alarm

**Step 1** Check that the provisioned circuit size is correct:

- Click the **Circuits** tab.
- Find the appropriate row using the Circuit Name and record the size listed in the size column.
- Determine whether the size listed matches the original network design plan.

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

- Click the circuit row to highlight it and click **Delete**.
- Click **Yes** at the Delete Circuits dialog box.
- Recreate the circuit with the correct circuit size.

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

- Measuring the source signal with a test set to determine if the circuit size matches the provisioned circuit.
- If the source circuit signal is a test set, check that the test set settings match the intended circuit size.

## 1.5.29 CONTBUS-A

- Major, Non-service affecting

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

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



### Caution

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

### Procedure: Clear the CONTBUS-A Alarm

- 
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type.
- Step 2** Click the **Inventory** tab to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, complete the [“Clear the MEA Alarm” procedure on page 1-74](#).
- Step 3** If only one card slot is reporting the alarm, perform a CTC reset of the traffic card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click and choose **RESET CARD**.
- Step 4** If the CTC reset does not clear the alarm, physically reseal the reporting card.
- Step 5** If all traffic cards report this alarm, perform a CTC reset of the active TCC+ card:
- Display the node view.
  - Position the cursor over the active TCC+ card slot.
  - Right-click and choose **RESET CARD**.
  - Click **Yes** when the “Are You Sure?” dialog box appears.
  - Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
  - Confirm that the TCC+ you reset is in standby mode after the reset:  
The TCC+ card’s LED will be amber for standby or green for active, or  
In node view, run the mouse over the TCC+ card and a pop up box will display if the card is active or standby.
- Step 6** If the CTC reset does not clear the alarm, physically reseal the TCC+ card.
- Step 7** If the alarm does not clear, replace the TCC+ card.

**Note**

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

## 1.5.30 CONTBUS-A-18

- Major, Non-service affecting

A Communication Failure from TCC Slot to TCC Slot alarm occurs when the main processor on the TCC+ card in Slot 7 loses communication with the coprocessor on the second TCC+ card in Slot 11. The problem is with the physical path of communication from the TCC+ card to the reporting card. The physical path of communication includes the two TCC+ cards and the backplane.

**Caution**

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

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

- Step 1** Position the cursor over the TCC+ card in Slot 7.
- Step 2** Right-click the mouse to reveal a menu.
- Step 3** To clear the alarm, choose **RESET CARD** to make the standby TCC+ in Slot 11 the active TCC+ and clear the alarm.
- Step 4** Wait approximately 2 minutes for the TCC+ in Slot 7 to reset as the standby TCC+. Verify that the Standby LED is lit before proceeding to the next step.
- Step 5** Position the cursor over the TCC+ card in Slot 11.
- Step 6** Right-click the mouse to reveal a menu.
- Step 7** Choose **RESET CARD** to make the standby TCC+ in Slot 7 the active TCC+.
- Step 8** If the alarm reappears when the TCC+ in Slot 7 reboots as the active TCC+, the TCC+ card in Slot 7 is defective and must be replaced.

**Note**

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

## 1.5.31 CONTBUS-B

- Major, Non-service affecting

A Communication Failure TCC B to Shelf Slot alarm occurs when the TCC+ card in Slot 11 loses communication with a traffic card. Cards require frequent communication with the TCC+ card, because the TCC+ card performs system initialization, provisioning, alarm reporting, maintenance, diagnostics,

IP address detection/resolution, SONET DCC termination, and system fault detection among other operations for the ONS 15454. The TCC+ card also ensures that the system maintains Telcordia timing requirements.

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

**Caution**

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

## Procedure: Clear the CONTBUS-B

- 
- Step 1** Ensure that the reporting card is physically present on the shelf and that it matches the type of card identified in that slot on CTC.
- Step 2** If this slot is the only slot reporting the alarm, perform a CTC reset of the traffic card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click the mouse and choose **RESET CARD**.
- Step 3** If the CTC reset does not clear the alarm, physically reseal the reporting card.
- Step 4** If all cards with the exception of the active TCC+ report this alarm, perform a CTC reset of the active TCC+:
- Display the node view.
  - Position the cursor over the active TCC+ card slot.
  - Right-click and choose **RESET CARD**.
  - Click **Yes** when the “Are You Sure?” dialog box appears.
  - Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
  - Confirm that the TCC+ you reset is in standby mode after the reset:
 

The TCC+ card’s LED will be amber for standby or green for active, or
  - In node view, run the mouse over the TCC+ card and a pop up box will display if the card is active or standby.
- Step 5** If the CTC reset does not clear the card, physically reseal the TCC+ card (see the [“Reset the TCC+ With a Card Pull”](#) section on page 3-5).
- Step 6** If the alarm does not clear, replace the TCC+ card.

**Note**

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

## 1.5.32 CONTBUS-B-18

- Major, Non-service affecting

A Communication Failure from TCC Slot to TCC Slot alarm occurs when the main processor on the TCC+ card in Slot 11 loses communication with the coprocessor on the TCC+ card in Slot 7. The problem is with the physical path of communication from the TCC+ card to the reporting TCC+ card. The physical path of communication includes the two TCC+ cards and the backplane.



### Caution

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

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

- 
- Step 1** Position the cursor over the TCC+ card in Slot 11.
- Step 2** Right-click and choose **RESET CARD** to make the TCC+ in Slot 11 the active TCC+ card.
- Step 3** Wait approximately 2 minutes for the TCC+ in Slot 7 to reset as the standby TCC+ card. Verify that the Standby LED is lit before proceeding to the next step.
- Step 4** Position the cursor over the TCC+ card in Slot 7.
- Step 5** Right-click and choose **RESET CARD** again to make the TCC+ in Slot 11 the active TCC+ card.
- Step 6** If the alarm reappears when the TCC+ in Slot 11 reboots as the active TCC+, the TCC+ card in Slot 11 is defective and must be replaced.



### Note

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

## 1.5.33 CTNEQPT-PBPROT

- Critical, Service affecting

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



### Note

If all traffic cards show this alarm, physically reseal the standby TCC+ card (see the [“Reset the TCC+ With a Card Pull”](#) section on page 3-5). If this fails to clear the alarm, replace the standby TCC+ card. Do not physically reseal an active TCC+ card. This disrupts traffic.



### Caution

It can take up to 30 minutes for software to be updated on a standby TCC+ card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

**Caution**

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

## Procedure: Clear the CTNEQPT-PBPROT Alarm

- 
- Step 1** Perform a CTC reset on the standby cross-connect (XC/XCVT/XC10G) card:
- Display the node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click and choose **RESET CARD**.
- Step 2** If the alarm persists, physically reseal the standby cross-connect card.
- Step 3** If the alarm persists and the reporting traffic card is the active card in the protection group, perform a force switch to move traffic away from the card:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Click the Protect/Standby card of the selected groups.
  - Click **Force** and **OK**.
- Step 4** Perform a CTC reset on the reporting card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click to choose **RESET CARD**.
- Step 5** If the alarm persists, physically reseal the reporting card.
- Step 6** Clear the force switch:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Highlight either selected group.
  - Click **Clear** and click **YES** at the confirmation dialog box.
- Step 7** If the reporting traffic card is protect, perform a CTC reset on the reporting card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click and choose **RESET CARD**.
- Step 8** If the alarm persists, physically reseal the reporting card.
- Step 9** If the alarm persists, replace the standby cross-connect card.

**Note**

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

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

**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 procedures.

## 1.5.34 CTNEQPT-PBWORK

- Critical, Service affecting

The Interconnection Equipment Failure Protect Payload Bus alarm indicates a failure in the main payload bus between the active cross-connect (XC/XCVT/XC10G) card in Slot 8 and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card, the reporting traffic card, or the backplane.

**Note**

If all traffic cards show this alarm, perform a force switch on the active TCC+ card and physically reseal this TCC+ card. If this fails to clear the alarm, replace the TCC+ card. Do not physically reseal an active TCC+ card; this disrupts traffic.

**Caution**

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

### Procedure: Clear the CTNEQPT-PBWORK Alarm

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

- Determine the active cross-connect card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.

**Note**

You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

- In the node view, select the **Maintenance > XC Cards** tabs.
- Click **Switch**.
- Click **Yes** on the Confirm Switch dialog box.

**Note**

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

**Step 2** Perform a CTC reset on the reporting card:

- From the node view, position the cursor over the slot reporting the alarm.
- Right-click to choose **RESET CARD**.

- Step 3** If the alarm persists, perform a card pull on the standby cross-connect card.
- Step 4** If the alarm persists and the reporting traffic card is the active card in the protection group, perform a force switch to move traffic away from the card:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Click the Protect/Standby card of the selected groups.
  - Click **Force** and **OK**.
- Step 5** Perform a CTC reset on the reporting card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click to choose **RESET CARD**.
- Step 6** If the alarm persists, physically reseal the reporting card.
- Step 7** Clear the force switch:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Highlight either selected group.
  - Click **Clear** and click **YES** at the confirmation dialog box.
- Step 8** If the reporting traffic card is protect, perform a CTC reset on the reporting card:
- Display the CTC node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click to choose **RESET CARD**.
- Step 9** If the alarm persists, physically reseal the reporting card.
- Step 10** If the alarm persists, replace 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 persists, replace the reporting traffic card.




---

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

---

## 1.5.35 DATAFLT

- Minor, Non-service affecting

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



**Caution**

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

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

## 1.5.36 DS3-MISM

- Not Alarmed (NA) (Condition)

The DS3 Frame Format Mismatch indicates a frame format mismatch on the DS3-12E card. The condition occurs when the provisioned line type and incoming signal frame format type do not match. For example, if the line type is set to C-BIT for a DS3-12E card, and the incoming signal's frame format is detected as M23 or UNFRAMED, then the ONS 15454 reports a DS3-MISM alarm. The alarm is not raised when the line type is set to AUTO PROVISION or UNFRAMED.

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

### Procedure: Clear the DS3-MISM

- Step 1** Go to the CTC card-level view for the reporting DS3-12E.
- Step 2** Click **Provisioning > Line** tabs.
- Step 3** For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal.
- Step 4** If the Line Type pull-down column does not match the expected incoming signal, select the correct Line Type on the pull down menu.
- Step 5** Click **Apply**.
- Step 6** If the alarm does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use a test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal.

## 1.5.37 EHBATVG-A

- Major, Service affecting

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

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

## 1.5.38 EHIBATVG-B

- Major, Service affecting

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

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

## 1.5.39 ELWBATVG-A

- Major, Service affecting

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

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

## 1.5.40 ELWBATVG-B

- Major, Service affecting

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

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

## 1.5.41 EOC

- Major, Non-service affecting

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



Warning

---

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

---



Warning

---

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

---

**Caution**

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

**Procedure: Clear the EOC Alarm**

- 
- Step 1** If an LOS alarm is also reported, first resolve the LOS alarm by following the troubleshooting procedure given for that alarm.
- Step 2** On the node reporting the alarm, check the physical connections from the cards to the fiber-optic cables that are configured to carry DCC traffic.
- Step 3** Verify that both ends of the fiber span have in-service ports by checking that the ACT LED on each OC-N card is illuminated.
- Step 4** Verify that the DCC is provisioned for the ports at both ends of the fiber span.
- Under the node view, click the **Provisioning > SONET DCC** tabs.
  - If the slot and port are listed under **SDCC Terminations**, the DCC is provisioned.
  - If the slot and port are not listed under the SDCC Terminations, click **Create**.
  - Click the OC-N card that links to the adjacent node.
  - Click **OK**.
  - Repeat tab at the adjacent nodes.
- Step 5** Verify that the OC-N port is active and in-service:
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.  
A green LED indicates an Active card. A yellow LED indicates a Standby card.
  - To determine whether the OC-N port is in In Service, double-click the card in CTC to display the card-level view.
  - Click the **Provisioning > Line** tabs.
  - Verify that the Status column lists the port as In Service.
  - If the Status column lists the port as Out of Service, click the column and choose **In Service**. Click **Apply**.
- Step 6** With a test set, check for signal failures on fiber terminations.

**Caution**

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

- Step 7** Measure power levels to verify that the budget loss is within the parameters of the receiver. See the [“Optical Card Transmit and Receive Levels” section on page 2-43](#).
- Step 8** Ensure that fiber connectors are securely fastened and properly terminated.
- Step 9** Reset the active TCC+:
- Display the node view.
  - Position the cursor over the active TCC+ card slot.
  - Right-click and choose **RESET CARD**.

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

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




---

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

---

**Step 11** Delete and recreate the problematic SDCC termination:

- a. Click the **Provisioning > SONET DCC** tabs.
- b. Highlight the problematic SDCC termination.
- c. Click **Delete**.
- d. Click **Yes** at confirmation dialog box.

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

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

---

## 1.5.42 EQPT

- Critical, Service affecting

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

If the EQPT alarm occurs with a BKUPMEMP alarm, follow the procedure “[Clear the BKUPMEMP Alarm](#)” section on page 1-21. This procedure will also clear the EQPT alarm.



**Caution**

---

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

---

### Procedure: Clear the EQPT Alarm

---

**Step 1** Perform a CTC reset on the reporting card.

- a. Display the CTC node view.
- b. Position the CTC cursor over the slot reporting the alarm.
- c. Right-click **RESET CARD**.

**Step 2** If the CTC reset fails to clear the alarm, physically reseal the card.

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



**Caution**

---

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

---

**Note**

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

## 1.5.43 EQPT-MISS

- Critical, Service affecting

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

**Caution**

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

### Procedure: Clear the EQPT-MISS Alarm

- Step 1** If the alarm is reported against the fan object, check that the fan-tray assembly is present.
- Step 2** If the fan-tray assembly is present, use the retractable handles embedded in the front of the fan tray to pull the fan-tray assembly forward several inches and then push the fan-tray assembly firmly back into the ONS 15454 shelf assembly and close the retractable handles.
- Step 3** If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the fan-tray assembly installation information in the *Cisco ONS 15454 Procedure Guide*.

## 1.5.44 E-W-MISMATCH

- Major, Service affecting

A Procedural Error Misconnect East/West Direction alarm occurs when nodes in a ring have an east slot/port misconnected to another east slot/port or a west slot/port misconnected to another west slot/port. In most cases, the user did not hook up the fibers correctly, or the ring provisioning plan was flawed. You can physically reconnect the cable to the correct slot/ports to clear the E-W-MISMATCH alarm. Alternately, you can delete and recreate the span in CTC to change the west line and east line designations. The CTC method will clear the alarm, but may change the traditional east-west node connection pattern of the ring.

**Note**

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

**Note**

The lower numbered slot on a node is traditionally labelled as the west slot and the higher numbered slot is labelled as the east slot. For example, Slot 6 is west and Slot 12 is east.

## Procedure: Clear the E-W-MISMATCH Alarm with a Physical Switch

- 
- Step 1** Diagram the ring setup, including nodes and spans, on a piece of paper or white board.
  - Step 2** Display the CTC network view and label each of the nodes on the diagram with the same name that appears on the network map.
  - Step 3** Double-click each span to reveal the node name/slot/port for each end of the span.
  - Step 4** Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 - Node2/Slot6/Port1 (2F BLSR OC48, Ring ID=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as *Slot 12/Port 1*. Label the Node 2 end of that same span *Slot 6/Port 1*.
  - Step 5** Repeat Steps 3 and 4 for each span on your diagram.
  - Step 6** Label the highest slot at each node *east* and the lowest slot at each node *west*.
  - Step 7** Look at the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span.
  - Step 8** If any span has an east-to-east or west-to-west connection, physically switch the fiber connectors from the card that does not fit the pattern to the card that will continue the pattern. This should clear the alarm.



### Note

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



### Warning

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



### Warning

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

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

- 
- Step 1** Log into the misconnected node. This is the node with both ring fibers misconnected; it is in the middle of the two nodes that have one of two ring fibers misconnected.
  - Step 2** Click the **Provisioning > Ring** tabs.
  - Step 3** From the row of information for the fiber span, write down the Node ID, Ring ID, and the Slot and Port in the east line list and west line list.
  - Step 4** Click the row from [Step 3](#) to select it and click **Delete**.
  - Step 5** Click **Create**.

- Step 6** Fill in the Ring ID and Node ID from the information collected in [Step 3](#).
  - Step 7** Change the West line pull-down menu to the slot/port you recorded for the East line in [Step 3](#).
  - Step 8** Change the East line pull-down menu to the slot/port you recorded for the West line in [Step 3](#).
  - Step 9** Click **OK**.
  - Step 10** Click **Yes** at the Ring Map Change dialog box.
  - Step 11** Click **Accept** at the new Ring Map.
- 

## 1.5.45 EXCCOL

- Minor, Non-service affecting

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

### Procedure: Clear the EXCCOL Alarm

Troubleshoot the network management LAN connected to the TCC+ card for excess collisions. You may need to contact the system administrator of the network management LAN to accomplish the following steps:

- Step 1** Verify that the network device port connected to the TCC+ card has a flow rate set to 10 Mb, half-duplex.
  - Step 2** Troubleshoot the network device connected to the TCC+ card and the network management LAN.
- 

## 1.5.46 EXERCISE-RING-FAIL

- Not Alarmed (NA) (Condition)

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

**Note**

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

---

### Procedure: Clear the EXERCISE-RING-FAIL Condition

- Step 1** Check for any LOS, LOF, or BLSR service-affecting alarms.
- Step 2** Troubleshoot any of these alarms.

**Step 3** Reissue the Exercise-Ring command.

---

## 1.5.47 EXERCISE-SPAN-FAIL

- Not Alarmed (NA) (Condition)

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



**Note**

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

---

### Procedure: Clear the EXERCISE-SPAN-FAIL Condition

---

- Step 1** Check for any LOS, LOF or BLSR service affecting alarms.
- Step 2** Troubleshoot any of these alarms.
- Step 3** Reissue the Exercise Span command.
- 

## 1.5.48 EXT

- Minor, Service affecting

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

### Procedure: Clear the EXT Alarm

---

- Step 1** Open the AIC card maintenance screen to gather further information about this alarm.
- Step 2** Perform your standard operating procedure for this environmental condition.
- 

## 1.5.49 FAILTOSW

- Not Alarmed (NA) (Condition)

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



## Procedure: Clear the FAILTOSW Condition

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



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

**Step 2** Replace the working DS-N card that is reporting the higher-priority alarm. This card is the working DS-N card using the 1:N card protection and not reporting FAILTOSW.

Replacing the working DS-N card reporting the higher-priority alarm, will allow traffic to revert back to this slot. This frees up the 1:N card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW alarm.



**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 procedures.



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

## 1.5.50 FAILTOSW-PATH

- Not Alarmed (NA) (Condition)

The Fail to Switch Path condition occurs when the working path does not switch to the protection path on a UPSR. Common causes of this alarm include a missing or defective protection card or a lockout set on one of the UPSR nodes.



**Caution**

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

## Procedure: Clear the FAILTOSW-PATH on a UPSR Configuration

- Step 1** Ensure that a lockout is not set on the UPSR:
- Display the CTC network view.
  - Right-click the span (the line between the nodes).
  - Click **Circuits**.
  - Under Switch State, confirm that Clear appears.

- e. If Clear does appear, perform Steps a – d at the next span.
- f. If Clear does not appear, click the **Switch all UPSR- circuits away** menu.
- g. Choose **Clear** and click **Apply**.
- h. Click **Yes** at the Confirm UPSR Switch Are You Sure? dialog box.
- i. Click **OK** at the next dialog box.

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



**Warning**

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



**Warning**

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

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

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

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

- a. At the node view, click the **Maintenance > Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Click the Protect/Standby card of the selected groups.
- d. Click **Manual** and **OK**.

**Step 6** Perform a CTC reset on the reporting card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click to choose **RESET CARD**.
- d. If the alarm persists, physically reseal the reporting card.

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

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

**Step 9** If you are unable to perform a switch, reseal the protect card.

**Step 10** Attempt another manual switch.

**Step 11** Clear the manual switch:

- a. At the node view, click the **Maintenance > Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Highlight either selected group.
- d. Click **Clear** and click **YES** at the confirmation dialog box.

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



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

## 1.5.51 FAILTOSWR

- Not Alarmed (NA) (Condition)

This fail to switch ring signals an automatic protection switching (APS) ring switch failure. FAILTOSWR clears when one of the following actions occurs: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as an SF or SD alarm) clears.



**Warning**

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



**Warning**

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

### Procedure: Clear the FAILTOSWR on a Four-Fiber BLSR Configuration

- Step 1** Check to see that every node expected to be part of the ring is listed in the ring map:
- Click the **Provisioning > Ring** tabs.
  - Highlight the row of the affected ring.
  - Click **Ring Map**.
  - Verify that a Node ID appears in the Ring Map for every node expected to be part of the ring.
- Step 2** Display the CTC network view.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** Log into the near-end node and click the **Ring > Provisioning** tabs.

- Step 5** Record the OC-N cards listed under West Line and East Line. Ensure these OC-N cards are active and in-service.
- Step 6** Verify fiber continuity to the ports on the recorded cards.
- Step 7** Verify that the correct port is in-service.



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

---

- Step 8** Use an optical test set to verify that a valid signal exists on the line.  
Test the line as close to the receiving card as possible.
- Step 9** Clean the fiber:
- a. Clean fiber according to local site practice.
  - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 10** Verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 2-43 lists these specifications.
- Step 11** Repeat Steps 6–10 for any other ports on the card.
- Step 12** Replace the protect standby OC-N card.



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

---

- Step 13** If the alarm does not clear after you replace the BLSR cards on this node one by one, follow Steps 4–12 for each of the nodes in the ring.
- Step 14** Log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- 

## 1.5.52 FAILTOSWS

- Not Alarmed (NA) (Condition)

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

Follow the procedure for "Clear the FAILTOSWR on a Four-Fiber BLSR Configuration" section on page 1-47.

## 1.5.53 FAN

- Critical, Service affecting

The failure of the cooling fan tray alarm indicates a problem with the fan-tray assembly. When the fan is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range. The fan tray contains six fans and needs a minimum of five working fans to properly cool the ONS 15454. However, even with five working fans, the fan tray can need replacement because a sixth working fan is required for extra protection against overheating.

**Caution**

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

## Procedure: Clear the FAN Alarm

- 
- Step 1** Check the condition of the air filter to see if it needs replacement.
- Step 2** If the filter is clean, take the fan-tray assembly out of the ONS 15454.
- Step 3** Reinsert the fan tray making sure the back of the fan tray connects to the rear of the ONS 15454.



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

---

- Step 4** If the fan does not run or the alarm persists, replace the fan tray.
- Step 5** If the replacement fan tray does not operate correctly, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- 

## 1.5.54 FE-AIS

- Not Alarmed (NA) (Condition)

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

## Procedure: Clear the FE-AIS Condition

- 
- Step 1** To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 may link to the main AIS alarm from an DS3XM-6 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm.
- Step 3** Clear the main alarm.
-

## 1.5.55 FE-DS1-MULTLOS

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-DS1-MULTLOS Condition

- 
- Step 1** To troubleshoot an FE condition/alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition/alarm.
- Step 3** Look up and troubleshoot the main alarm.
- 

## 1.5.56 FE-DS1-SNGLLOS

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-DS1-SNGLLOS Condition

- 
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm.
- Step 3** Look up and troubleshoot the main alarm.
- 

## 1.5.57 FE-DS3-SA

- Not Alarmed (NA) (Condition)

The Far End DS3 Equipment Failure Service Affecting alarm occurs when a far-end DS-3 equipment failure occurs. The prefix FE in an alarm/condition means the main alarm is occurring at the far-end node and not at the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

## Procedure: Clear the FE-DS3-SA Condition

- 
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Clear the main alarm.
- 

## 1.5.58 FE-EQPT-NSA

- Not Alarmed (NA) (Condition)

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

**Caution**

---

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

---

## Procedure: Clear the FE-EQPT-NSA Condition

- 
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Look up and troubleshoot the main alarm.
- 

## 1.5.59 FE-IDLE

- Not Alarmed (NA) (Condition)

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

## Procedure: Clear the FE-IDLE Condition

- 
- Step 1** To troubleshoot the FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Clear the main alarm.
- 

## 1.5.60 FE-LOCKOUT

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-LOCKOUT Condition on a BLSR

- 
- Step 1** Display CTC network view.
- Step 2** Find the node reporting the LOCKOUT-REQ.
- Step 3** Log into the node reporting the LOCKOUT-REQ.
- Step 4** Follow the [“Clear the Lockout Switch Request and the LOCKOUT-REQ Condition” procedure on page 1-58.](#)
- 

## 1.5.61 FE-LOF

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-LOF Condition

- 
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE alarm.
- Step 3** Look up and troubleshoot the main alarm.
-



## 1.5.62 FE-LOS

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the FE-LOS Condition

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To troubleshoot the FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2. |
| <b>Step 2</b> | Log into the node that links directly to the card reporting the FE alarm.   |
| <b>Step 3</b> | Clear the main alarm.   |
- 

## 1.5.63 FEPRLF

- Minor, Non-service affecting

The Far End Protection Line Failure alarm occurs when an APS switching channel signal failure occurs on the protect card coming into the node.

**Note**

---

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

---

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

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE alarm/condition on a card in Slot 12 of Node 1 may link to the main alarm from a card in Slot 6 of Node 2. |
| <b>Step 2</b> | Log into the node that links directly to the card reporting the FE alarm.   |
| <b>Step 3</b> | Look up and troubleshoot the main alarm.  |
- 

## 1.5.64 FORCED-REQ

- Not Alarmed (NA) (Condition)

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

## Procedure: Clear the FORCED-REQ

- 
- Step 1** Click the **Maintenance** tab.
  - Step 2** Click the **Protection** tab for a card or span switch.
  - Step 3** At **Operation**, click the drop-down arrow.
  - Step 4** Choose **Clear** and click **Apply**.
- 

## 1.5.65 FRNGSYNC

- Major, Service affecting

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

## Procedure: Clear the FRNGSYNC Alarm

- 
- Step 1** If the ONS 15454 is configured to operate from its own internal clock, disregard this alarm.
  - Step 2** If the ONS 15454 is configured to operate off an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards.
  - Step 3** Find and troubleshoot alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI and SYNCSEC.
- 

## 1.5.66 FSTSYNC

- Minor, Non-service affecting

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




---

**Note** This is an informational alarm.

---

## 1.5.67 HITEMP

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

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

**Caution**

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

**Procedure: Clear the HITEMP Alarm**

- 
- Step 1** Check the temperature of the ONS 15454 on the front panel LCD.
  - Step 2** Check that the temperature of the room is not abnormally high.
  - Step 3** Ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454.
  - Step 4** Ensure that blank faceplates fill the ONS 15454 empty slots. Blank faceplates help airflow.
  - Step 5** Check the condition of the air filter to see if it needs replacement.
  - Step 6** If the filter is clean, take the fan-tray assembly out of the ONS 15454.
  - Step 7** Reinsert the fan tray, making sure the back of the fan tray connects to the rear of the ONS 15454.



---

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

---

- Step 8** If the fan does not run or the alarm persists, replace the fan tray.
  - Step 9** If the replacement fan tray does not operate correctly, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- 

## 1.5.68 HLDOVERSYNC

- Major, Service affecting

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

**Procedure: Clear the HLDOVERSYNC Alarm**

- 
- Step 1** Check for additional alarms that relate to timing.
  - Step 2** Reestablish a primary and secondary timing source according to local site practice.
- 

## 1.5.69 IMPROPRMVL

- Critical, Service-affecting

The Improper Removal alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in-service to cause this alarm, it only needs to be recognized by CTC and the TCC+ card. This alarm does not appear if you delete the card from CTC before you physically remove the card from the node.

**Note**

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

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

**Caution**

Do not pull a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot.

**Caution**

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

## Procedure: Clear the IMPROPRMVL Alarm

**Step 1** Right-click the card reporting the IMPROPRMVL.

**Step 2** Choose **Delete**.

**Note**

CTC will not allow you to delete this card if the card is in-service, has a circuit mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

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

**Caution**

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

- a. In CTC, double-click the reporting card to display the card view.
- b. Click the **Provisioning** tab.
- c. Click the **Status** of any in-service ports.
- d. Choose **Out of Service** to take the ports out of service.

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

**Caution**

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

- a. At the node view, click the **Circuits** tab.
- b. Click the applicable circuit, i.e., the circuit that connects to the reporting card.

- c. Click **Delete**.
- Step 5** If the card is paired in a protection scheme, delete the protection group:
- a. Click the **Provisioning > Protection** tabs.
  - b. Click the protection group of the reporting card.
  - c. Click **Delete**.
- Step 6** If the card is provisioned for DCC, delete the DCC provisioning:
- a. Click the **SONET DCC > Provisioning** tabs.
  - b. Click the slots and ports listed in SDCC Terminations.
  - c. Click **Delete** and click **Yes** in the dialog box that appears.
- Step 7** If the card is used as a timing reference, change the timing reference:
- a. Click the **Provisioning > Timing** tabs.
  - b. Click the **Ref-1** menu.
  - c. Change Ref-1 from the listed OC-N card to Internal Clock.
  - d. Click **Apply**.
- Step 8** Right-click the card reporting the IMPROPRMVL and choose **Delete**.
- 

## 1.5.70 INCOMPATIBLE-SW

- Minor, Non-service affecting

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

### Procedure: Clear the INCOMPATIBLE-SW Alarm

**Note**

See also the [“Operation: Different CTC Releases Do Not Recognize Each Other”](#) section on page 2-23.

---

- Step 1** Exit the current CTC session and completely close the browser.
- Step 2** Start the browser.
- Step 3** Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.
- Step 4** Log into CTC. The browser will download the jar file from CTC.
-

## 1.5.71 INVMACADDR

- Major, Non-service affecting

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

### Procedure: Clear the INVMACADDR Alarm

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

## 1.5.72 KB-PASSTHR

- Not Alarmed (NA) (Condition)

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

### Procedure: Clear the KB-PASSTHR Condition

- 
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
  - Step 2** In the node (default CTC login view), click the **Maintenance > BLSR** tabs.
  - Step 3** Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.
  - Step 4** Choose **CLEAR** and click **Apply**.
  - Step 5** Click **OK** on the BLSR Operations dialog box.

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

---

## 1.5.73 LOCKOUT-REQ

- Not Alarmed (NA) (Condition)

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

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

- 
- Step 1** Display the CTC network view.

- Step 2** Click **Circuits** tab and highlight the circuit.
- Step 3** Click **Edit** and click the **UPSR** tab.
- Step 4** From the Switch State menu, highlight **Clear**.
- Step 5** Click **Apply** and click **Close**.

## 1.5.74 LOF (BITS)

- Major, Service affecting

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



### Note

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



### Caution

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

## Procedure: Clear the LOF Alarm

- Step 1** Verify that the line framing and line coding match between the BITS input and the TCC+:
- In CTC node view or card view, note the slot and port reporting the alarm.
  - Find the coding and framing formats of the external BITS timing source. This should be in the user documentation for the external BITS timing source or on the timing source itself.
  - Click the **Provisioning > Timing** tabs to display the General Timing screen.
  - Verify that **Coding** matches the coding of the BITS timing source (either B8ZS or AMI).
  - If the coding does not match, click **Coding** to reveal a menu. Choose the appropriate coding.
  - Verify that **Framing** matches the framing of the BITS timing source (either ESF or SF [D4]).
  - If the framing does not match, click **Framing** to reveal the menu. Choose the appropriate framing.



### Note

On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field, and the AMI coding field is normally paired with SF (D4) in the Framing field.

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

**Note**

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

## 1.5.75 LOF (DS1)

- Major, Service affecting

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

### Procedure: Clear the LOF Alarm

- Step 1** Verify that the line framing and line coding match between the DS1-14 port and the signal source.
- In CTC, note the slot and port reporting the alarm.
  - Find the coding and framing formats of the signal source for the card reporting the alarm. You may need to contact your network administrator for this information.
  - Display the card-level view of the reporting card.
  - Click the **Provisioning > Line** tabs.
  - Verify that the line type of the reporting port matches the line type of the signal source.
  - If the signal source line type does not match the reporting port, click **Line Type** to reveal a menu. Choose the matching type.
  - Verify that the reporting Line Coding matches the signal source's Line Type.
  - If the signal source line coding does not match the reporting port, click **Line Coding** to reveal the menu. Choose the matching type and click **Apply**.

**Note**

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

**Note**

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

## 1.5.76 LOF (DS3)

- Critical, Service affecting



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

## Procedure: Clear the LOF Alarm

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

### 1.5.77 LOF (EC1-12)

- Critical, Service affecting

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

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



#### Caution

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

## Procedure: Clear the LOF Alarm

- Step 1** The LOF should trigger an automatic protection switch away from the working card that reported the alarm. If it did not, perform a manual switch to move traffic away from the reporting card:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Click the Protect/Standby card of the selected groups.
  - Click **Manual** and **OK**.

- Step 2** Clear the manual switch:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Highlight either selected group.
  - Click **Clear** and click **YES** at the confirmation dialog box.



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

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

## 1.5.78 LOF (OC-N)

- Critical, Service affecting

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

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



### Caution

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

### Procedure: Clear the LOF Alarm

- Step 1** The LOF should trigger an automatic protection switch away from the working card that reported the alarm. If it did not, perform a manual switch to move traffic away from the reporting card:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Click the Protect/Standby card of the selected groups.
  - Click **Manual** and **OK**.



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

- Step 2** Clear the manual switch:
- At the node view, click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Highlight either selected group.
  - Click **Clear** and click **YES** at the confirmation dialog box.
- Step 3** Verify that the OC-N port on the upstream node is in-service.
- Step 4** If you continue to receive the LOF alarm, see the [“Optical Card Transmit and Receive Levels” section on page 2-43](#).

## 1.5.79 LOGBUFR90

- Major, Service affecting

The Log Buffer 90% Full alarm occurs when the memory buffer holding the raised alarms is 90% full. If the buffer continues to fill, a LOGBUFROVFL alarm is reported. The LOGBUFROVFL alarm occurs when the memory buffer is full, and any new alarms occurring on the ONS 15454 will not display on the CTC Alarms tab. CTC receives alarms from all ONS nodes on the network, even if CTC is in the node view or card view.

### Procedure: Clear the LOGBUFR90 Alarm

- 
- Step 1** Click the Close button on the upper right corner of the CTC screen.
- Step 2** Click the Close button on the upper right corner of the browser screen.
- Step 3** Log back into the ONS 15454. The LOGBUFR90 alarm should clear after approximately one minute. Exiting CTC and logging back into the ONS 15454 removes any cleared alarms from the log buffer and resynchronizes the alarm pane to show any alarms that were not displayed as a result of a full log buffer.



---

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

---

## 1.5.80 LOGBUFROVFL

- Major, Service affecting

The Log Buffer Overflow alarm occurs when the memory buffer is full; any new alarms occurring on the ONS 15454 will not display on the CTC Alarms tab. CTC receives alarms from all ONS nodes on the network, even if CTC is displaying the node view or card view.

### Procedure: Clear the LOGBUFROVFL Alarm

- 
- Step 1** Click the close button on the upper right corner of the CTC screen.
- Step 2** Click the close button on the upper right corner of the browser screen.
- Step 3** Log back into the ONS 15454. The LOGBUFROVFL alarm should clear after an approximately one minute delay. Exiting CTC and logging back into the ONS 15454 removes any cleared alarms from the log buffer and resynchronizes the Alarm tab to show any alarms not displayed as a result of a full log buffer.



---

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

---

## 1.5.81 LOP-P

- Critical, Service affecting

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

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

**Caution**

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

## Procedure: Clear the LOP-P Alarm

- 
- Step 1** Verify the cabling and physical connections on the reporting card.
- Step 2** Perform a CTC reset on the reporting card:
- a. Display the CTC node view.
  - b. Position the cursor over the slot reporting the alarm.
  - c. Right-click to choose **RESET CARD**.
- Step 3** Perform a manual switch (side switch) to move traffic away from the card.
- a. At the node view, click the **Maintenance > Protection** tabs.
  - b. Double-click the protection group that contains the reporting card.
  - c. Click the Protect/Standby card of the selected groups.
  - d. Click **Manual** and **OK**.



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

---

- Step 4** Clear the manual switch:
- a. At the node view, click the **Maintenance > Protection** tabs.
  - b. Double-click the protection group that contains the reporting card.
  - c. Highlight either selected group.
  - d. Click **Clear** and click **YES** at the confirmation dialog box.
- Step 5** If the alarm persists, the problem is at the far-end node. Verify the stability of the cabling and physical connections that connect to the far-end card.
- Step 6** Perform a CTC reset on the far-end card:
- a. Display the CTC node view.
  - b. Position the cursor over the slot reporting the alarm.
  - c. Right-click and choose **RESET CARD**.
- Step 7** Perform a CTC reset on the reporting card:
- a. Display the CTC node view.

- b. Position the cursor over the slot reporting the alarm.
- c. Right-click and choose **RESET CARD**.

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

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



**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 procedures.



**Note**

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

## 1.5.82 LOP-V

- Major, Service affecting

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



**Caution**

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

### Procedure: Clear the LOP-V Alarm

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

**Step 2** Perform a CTC reset on the reporting card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click and choose **RESET CARD**.

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

- a. At the node view, click the **Maintenance > Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Click the Protect/Standby card of the selected groups.
- d. Click **Manual** and **OK**.




---

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

---

- Step 4** Clear the manual switch:
- a. At the node view, click the **Maintenance > Protection** tabs.
  - b. Double-click the protection group that contains the reporting card.
  - c. Highlight either selected group.
  - d. Click **Clear** and click **YES** at the confirmation dialog box.
- Step 5** If the alarm persists, the problem is at the far-end node. Verify the cabling and physical connections that connect to the far-end card.
- Step 6** Perform a CTC reset on the far-end card.
- Step 7** Switch from the far-end working card to the far-end protect card.
- 

## 1.5.83 LOS (BITS)

- Major, Service affecting

The TCC+ card has a loss of signal (LOS) from the BITS timing source. An LOS occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.

**Caution**


---

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

---

### Procedure: Clear the LOS Alarm

- 
- Step 1** Verify the wiring connection from the ONS 15454 backplane BITS clock pin fields to the timing source.
- Step 2** Check that the BITS clock is operating properly.
- 

## 1.5.84 LOS (DS-N)

- Critical, Service affecting

A Loss of Signal for either a DS-3 port or a DS1-14 port occurs when the port on the card is in-service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

**Caution**


---

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

---

## Procedure: Clear the LOS Alarm

- 
- Step 1** Verify cabling continuity to the port.
- Step 2** Verify that the correct port is in-service.
- Step 3** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible.
- Step 4** Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.
- Step 5** If there is a valid signal, replace the DS-N connector on the ONS 15454.
- Step 6** Repeat Steps 1–5 for another port on the card.
- Step 7** Look for another alarm that may identify the source of the problem.
- Step 8** Replace the reporting card.

**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 procedures.

**Note**

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

## 1.5.85 LOS (EC1-12)

- Critical, Service affecting

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

**Caution**

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

## Procedure: Clear the LOS Alarm

- 
- Step 1** Verify cabling continuity to the port.
- Step 2** Verify that the correct port is in-service.
- Step 3** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible.
- Step 4** Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

**Step 5** If there is a valid signal, replace the cable connector on the ONS 15454.

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

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

**Step 8** Replace the reporting card.

**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 procedures.

**Note**

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

## 1.5.86 LOS (OC-N)

- Critical, Service affecting

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

**Warning**

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

**Warning**

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

**Caution**

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

### Procedure: Clear the LOS Alarm

**Step 1** Verify fiber continuity to the port.

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

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



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

- Step 4** Clean the fiber:
- a. Clean fiber according to local site practice.
  - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that the power level of the optical signal is within the OC-N card's receiver specifications. The [“Optical Card Transmit and Receive Levels” section on page 2-43](#) lists these specifications for each card.
- Step 6** If there is a valid signal, replace the connector on the backplane.
- Step 7** Repeat Steps 1–6 for another port on the card.
- Step 8** 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 procedures.

## 1.5.87 LPBKDS1FEAC

- Not Alarmed (NA) (Condition)

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

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information about loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

**Caution**

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

**Note**

This is an informational alarm.

## 1.5.88 LPBKDS3FEAC

- Not Alarmed (NA) (Condition)

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

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information about loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

**Caution**

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

**Note**

This is an informational alarm.

## 1.5.89 LPBKFACILITY (DS-N or EC1-12)

- Not Alarmed (NA) (Condition)

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information on loopbacks, see [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

There are two types of loopbacks: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. You can provision loopbacks through CTC.

**Caution**

The CTC permits loopbacks to be performed on an in-service circuit. This operation is service affecting.

**Note**

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

### Procedure: Clear the LBKFACILITY Condition

- 
- Step 1** From the node view, double-click the reporting card.
- Step 2** Click the **Maintenance** tab.
- If the condition is reported against a DS3XM-6 card, also click the **DS1** tab.
  - If a Loopback Type column cell that displays Facility (Line) is not shown under the **DS1** tab, then click the **DS3** tab to reveal a Loopback Type column cell that displays Facility (Line).
- Step 3** Click the Loopback Type column cell that displays Facility (Line).
- Step 4** Click **None**, and click **Apply**.
-

## 1.5.90 LPBKFACILITY (OC-N)

- Not Alarmed (NA) (Condition)

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly-used troubleshooting technique. A signal is sent out on a link or section of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network section. By setting up loopbacks on various parts of the network and excluding other parts, you can logically isolate the source of the problem. For more information on loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far end equipment. You provision loopbacks using CTC.

**Caution**

Before performing a facility loopback on an OC-N card, make sure the card contains at least two SDCC paths to the node where the card is installed. A second SDCC path provides a non-looped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second SDCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N.

### Procedure: Clear the LBKFACILITY Condition

- 
- Step 1** To remove the loopback alarm, double-click the reporting card in CTC.
  - Step 2** Click the **Maintenance** tab.
  - Step 3** Click the Loopback Type column and choose **None** from the menu.
  - Step 4** Click **Apply**.
- 

## 1.5.91 LPBKTERMINAL (DS-N, EC1-12)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly-used troubleshooting technique. A signal is sent out on a suspect link or part of the network, and a signal comes back to the sending device. If the signal does not come back or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically isolate the source of the problem. For more information on loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far end equipment. You provision loopbacks using CTC.

**Note**


---

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

---

## Procedure: Clear the LBKTERMINAL Condition

---

- Step 1** To remove the loopback alarm, double-click the reporting card in CTC.
- Step 2** Click the **Maintenance** tab.
- Step 3** Click the Loopback Type column and choose **None** from the menu.
- Step 4** Click **Apply**.
- 

### 1.5.92 LPBKTERMINAL(G1000-4)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software terminal loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter logically isolates the source of the problem. For more information on loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

When a port is set in terminal loopback the outgoing signal being transmitted is fed back into the receive direction on the same port and the externally received signal is ignored. On the G1000-4 card the outgoing signal is not transmitted; it is only fed back to the receive direction. G1000-4 cards only support Terminal loopbacks. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. Loopbacks are provisioned using CTC. CTC permits loopbacks on an in-service circuit. This operation is service affecting.

## Procedure: Clear the LPBKTERMINAL Condition

---

- Step 1** To remove the loopback alarm, double-click the reporting card in CTC.
- Step 2** Click the **Maintenance** tab.
- Step 3** Choose the Loopback Type column and choose **None** from the menu.
- Step 4** Click **Apply**.
- 

### 1.5.93 LPBKTERMINAL (OC-N)

- Not Alarmed (NA) (Condition)

A Loopback Terminal condition occurs when a software facility loopback is active for a port on the reporting card.

Loopback is a commonly-used troubleshooting technique. A signal is sent out on a suspect link or part of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link or network part. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically isolate the source of the problem. For more information on loopbacks, see the [“Identify Points of Failure on a Circuit Path” section on page 2-3](#).

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far end equipment. You provision loopbacks using CTC.

### Procedure: Clear the LBKTERMINAL Condition

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To remove the loopback alarm, double-click the reporting card in CTC. |
| <b>Step 2</b> | Click the <b>Maintenance</b> tab.                                     |
| <b>Step 3</b> | Click the Loopback Type column and choose <b>None</b> from the menu.  |
| <b>Step 4</b> | Click <b>Apply</b> .  |
- 

## 1.5.94 MAN-REQ

- Not Alarmed (NA) (Condition)

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

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

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | From network view, click the <b>Circuits</b> tab.    |
| <b>Step 2</b> | Highlight the circuit.                               |
| <b>Step 3</b> | Click <b>Edit</b> and click the <b>UPSR</b> tab.     |
| <b>Step 4</b> | From the Switch State menu, highlight <b>Clear</b> . |
| <b>Step 5</b> | Click <b>Apply</b> and click <b>Close</b> .          |
- 

## 1.5.95 MANRESET

- Not Alarmed (NA) (Condition)

A Manual System Reset condition occurs when you right-click a card in CTC and choose **Reset**. Resets performed during a software upgrade also prompt the alarm. This condition clears automatically, when the card finishes resetting.

## 1.5.96 MEA (AIP)

- Critical, Service affecting

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

### Procedure: Clear the MEA Alarm

Follow the [“Replace the Alarm Interface Panel”](#) section on page 3-15.

## 1.5.97 MEA (EQPT)

- Critical, Service affecting

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

### Procedure: Clear the MEA Alarm

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

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

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




---

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

---

- Step 2** Physically verify the type of card that sits in the slot reported in the object column of the MEA row on the alarms screen by reading the name at the top of the card's faceplate.
- If you have a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to [Step 3](#).
  - If you have a newer ANSI 10 Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed.



**Note** The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10 Gbps compatible shelf assembly and are the functional equivalent of the older, non-compatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a ANSI 10 Gbps compatible shelf assembly.

- c. If you have an older, pre-ANSI shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the XC10G, OC-192, E1000-2-G, E100T-G or OC-48 any slot (AS), proceed to [Step 3](#).
- d. If you have an older, pre-ANSI shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the XC10G, OC-192, E1000-2-G, E100T-G or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed.

**Step 3** On CTC, click the **Inventory** tab to reveal the provisioned card type.

**Step 4** If you prefer the card type depicted by CTC, replace the physical card reporting the mismatch with the card type depicted by CTC (provisioned for that slot).



**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 procedures.

**Step 5** If you prefer the card that physically occupies the slot and the card is not in-service, has no circuits mapped to it and is not part of a protection group, then put the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.



**Note** If the card is in-service, has a circuit mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, then CTC will not allow you to delete the card.

**Step 6** If the card is in-service, take the facility out of service:



**Caution** Before taking the facility out of service, ensure that no live traffic exists on the facility.

- a. Double-click the reporting card to display the card view.
- b. Click the **Provisioning** tab.
- c. Click the **Status** of any in-service ports.
- d. Choose **Out of Service** to take the ports out of service.

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



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

- a. On the node view, click the **Circuits** tab.
- b. Choose the applicable circuit (the one that connects to the reporting card).

- c. Click **Delete**.

**Step 8** If the card is paired in a protection scheme, delete the protection group:

- a. Click the **Provisioning > Protection** tabs.
- b. Choose the protection group of the reporting card.
- c. Click **Delete**.

**Step 9** Right-click the card reporting the alarm.

**Step 10** Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

---

## 1.5.98 MEA (FAN)

- Critical, Service affecting

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

### Procedure: Clear the MEA Alarm

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

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

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

**Step 2** If you have a 15454-SA-ANSI shelf or 10 Gbps compatible shelf assembly, the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. See the [“Replace the Fan-Tray Assembly” section on page 3-13](#).

**Step 3** If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and see the [“Replace the Fan-Tray Assembly” section on page 3-13](#).

---

## 1.5.99 MEM-GONE

- Major, Non-service affecting



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

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

## 1.5.100 MEM-LOW

- Minor, Non-service affecting

The free memory of card almost gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC+ card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC+ card is exceeded, CTC will cease to function.

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

## 1.5.101 MFGMEM

- Critical, Service Affecting

The MFGMEM or Manufacturing Data Memory Failure alarm raises if the ONS 15454 cannot access the data in the erasable programmable read-only memory (EPROM). Either the memory module on the component failed or the TCC+ lost the ability to read that module. The EPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address will disrupt IP connectivity and gray out the ONS 15454 icon on the CTC network view.

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

- 
- Step 1** Perform a CTC reset on the TCC+ card:
- In node view, run the mouse over the TCC+ card and a pop up box will display if the card is active or standby.
  - Position the cursor over the active TCC+ card slot.
  - Right-click and choose **RESET CARD**.
  - Click **Yes** when the “Are You Sure?” dialog box appears.
  - Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
  - Confirm that the TCC+ you reset is in standby mode after the reset:  
The TCC+ card’s LED will be amber for standby or green for active, or  
In node view, run the mouse over the TCC+ card and a pop up box will display whether the card is active or standby.
- Step 2** If the alarm does not clear, perform a card pull reset on the TCC+ by referring to the [“Reset the TCC+ With a Card Pull”](#) section on page 3-5.

- Step 3** If the alarm does not clear, physically replace the standby TCC+ card on the ONS 15454 with a new TCC+ card.
- Open the TCC+ card ejectors.
  - Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.
  - Open the ejectors on the TCC+ card.
  - Slide the TCC+ card into the slot along the guide rails.
  - Close the ejectors.




---

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

---

- Step 4** Right-click the active TCC+ card to reveal a pull-down menu.
- Step 5** Click **Reset Card**.
- Wait for the TCC+ to reboot. The ONS 15454 switches the standby TCC+ card to active mode.
- Step 6** Verify that the remaining TCC+ card is now in standby mode (the ACT/STBY LED changes to amber).
- Step 7** Physically replace the remaining TCC+ card with the second TCC+ card.
- Open the TCC+ card ejectors.
  - Slide the card out of the slot.
  - Open the ejectors on the TCC+ card.
  - Slide the TCC+ card into the slot along the guide rails.
  - Close the ejectors.
- The ONS 15454 boots up the second TCC+ card. The second TCC+ must also copy the system software, which can take up to twenty minutes.
- Step 8** If the MFGMEM alarm continues to report after replacing the TCC+ cards, the problem lies in the EPROM.
- Step 9** If the MFGMEM is reported from the fan tray, replace the fan tray.
- Step 10** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan tray is replaced, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
- 

## 1.5.102 NOT-AUTHENTICATED

- Minor, Non-service affecting

This not authenticated alarm indicates that the username and password entered do not match the information stored in the TCC+. All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For more information see the “[Operation: Username or Password Do Not Match](#)” section on page 2-24.

**Note**

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

## Procedure: Clear the NOT-AUTHENTICATED Alarm

- 
- Step 1** If you have an alternate username and a password available to access the system:
- Use the alternate username and password to access the ONS node.
  - Click the **Provisioning > Security** tabs.
  - Look under the Users field to find the username that raised the alarm.
  - If the username that raised the alarm is listed, then highlight the username to reveal the associated password. Record the correct password.
  - If the username is not listed, then click **Create**.
  - Fill in the fields on the Create User dialog box with the username and password that raised the alarm then click **OK**.
- Step 2** If you do not have an alternate username and password available, call the Cisco Technical Assistance Center at (1-800-553-2447). TAC can issue a new username and password.
- 

## 1.5.103 PDI-P

- Not Alarmed (NA) (Condition)

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

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

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

**Warning**

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

**Warning**


---

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

---

**Caution**


---

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

---

## Procedure: Clear the PDI-P Condition

- 
- Step 1** Verify that all circuits terminating in the reporting card are in an active state:
- a. Click the **Circuits** tab.
  - b. Verify that the State column lists the port as ACTIVE.
  - c. If the State column lists the port as INCOMPLETE, wait 10 minutes for the ONS 15454 to fully initialize. If INCOMPLETE does not change after full initialization, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- Step 2** After determining that the port is active, ensure that the signal source to the card reporting the alarm is working.
- Step 3** If traffic is affected, delete and recreate the circuit.




---

**Caution** Deleting a circuit may affect traffic.

---

- Step 4** Check the far-end OC-N card that provides STS payload to the reporting card.
- Step 5** Confirm the cross-connect between the OC-N card and the reporting card.
- Step 6** Clean the far-end optical fiber:
- a. Clean the fiber according to local site practice.
  - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 7** Replace the optical/electrical cards.

**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 procedures.

---

**Note**


---

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

---

## 1.5.104 PEER-NORESPONSE

- Major, Non-service affecting

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

### Procedure: Clear the PEER-NORESPONSE Alarm Reported

- 
- Step 1** On the node view, right-click the card reporting the alarm.
- Step 2** Click **Reset Card** and **OK** on the confirmation dialog.
- Step 3** Wait for the card to reset.
- Step 4** At reset, the green Act LED on the card will be replaced on CTC by a white Ldg LED. When the card finishes resetting, the green Act LED will reappear.
- Step 5** Right-click the peer card of the card reporting the alarm.
- Step 6** Click **Reset Card** and **OK** on the confirmation dialog.
- 

## 1.5.105 PLM-P

- Critical, Service affecting

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

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



**Warning**

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



**Warning**

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



**Caution**

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

## Procedure: Clear the PLM-P Alarm

- 
- Step 1** Verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
  - Verify that the State column lists the port as ACTIVE.
  - If the State column lists the port as INCOMPLETE, wait 10 minutes for the ONS 15454 to fully initialize. If INCOMPLETE does not change after full initialization, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- Step 2** After determining the port is active, verify the signal source to the traffic card reporting the alarm.
- Step 3** If traffic is being affected, delete and recreate the circuit.



**Caution** Deleting a circuit may affect traffic.

---

- Step 4** Verify that the far-end OC-N card that provides STS payload to the DS-N card.
- Step 5** Verify the cross-connect between the OC-N card and the DS-N card.
- Step 6** Clean the far-end optical fiber:
- Clean the fiber according to local site practice.
  - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 7** Replace the OC-N/DS-N cards.



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

---



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

---

## 1.5.106 PLM-V

- Minor, Service affecting

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

## Procedure: Clear the PLM-V Alarm

- 
- Step 1** Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.
- Step 2** Verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.
- 

## 1.5.107 PRC-DUPID

- Major, Service affecting

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

## Procedure: Clear the PRC-DUPID Alarm

- 
- Step 1** Find the nodes with identical node IDs.
- a. Log into a node on the ring.
  - b. Click the **Provisioning > Ring** tabs.
  - c. Record the Node ID number.
  - d. Repeat these substeps for all the nodes on the ring.
- Step 2** If two nodes have an identical node ID number, change the node ID number of one node.
- a. Log into a node that has an identical node ID number.
  - b. Click the **Provisioning > Ring** tabs.
  - c. Change the number in the Node ID field to a unique number between 0 and 31.
  - d. Click **Apply**.
- 

## 1.5.108 PWR-A

- Major, Service-affecting

The NE Power Failure At Connector A alarm applies to the network element (NE) rack. It is raised when there is no power supplied to the main power connector. This alarm can be raised if power is connected to the backup power connector (Connector B) but not to Connector A, since power must be applied to both supplies.



**Warning**

---

**Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects will heat up and can cause serious burns or weld the metal object to the terminals.**

---

## Procedure: Clear the PWR-A Alarm

- 
- Step 1** Verify whether a power connection between the power source and power connector A is present.
  - Step 2** Verify and reseal, if necessary, the connections between the source and the power connector A.
  - Step 3** If the alarm cannot be cleared, verify the continuity of the power connection with a multimeter.
  - Step 4** If the alarm cannot be cleared, verify the source power output with a multimeter.
- 

## 1.5.109 PWR-B

- Major, Service-affecting

The NE Power Failure at Connector B alarm applies to the NE rack. It is raised when there is no power supplied to the backup power connector. This alarm can be raised if power is connected to the main power connector (Connector A) but not to Connector B, since power must be applied to both supplies.



**Warning**

---

**Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects will heat up and can cause serious burns or weld the metal object to the terminals.**

---

## Procedure: Clear the PWR-B Alarm

- 
- Step 1** Check whether a power connection is present between the power source and power connector B.
  - Step 2** Check and reseal, if necessary, the connections between the source and power connector B.
  - Step 3** If the alarm cannot be cleared, check the continuity of the power connection with a multimeter.
  - Step 4** If the alarm cannot be cleared, check power output from the source with a multimeter.
- 

## 1.5.110 RAI

- Not Alarmed (NA) (Condition)

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other.

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

## Procedure: Clear the RAI Condition

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



## 1.5.111 RCVR-MISS

- Major, Service affecting

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


**Note**

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


**Caution**

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

### Procedure: Clear the RCVR-MISS Alarm

- 
- Step 1** Ensure that the device attached to the DS1-14 port is operational.
  - Step 2** Verify that the cabling is securely connected.
  - Step 3** Verify that the pinouts are correct.
  - Step 4** Replace the receive cable if Steps 1 – 3 do not clear the alarm.
- 

## 1.5.112 RDI-P

See the “RFI-P” section on page 1-86.

## 1.5.113 RFI-L

- Not reported

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

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

### Procedure: Clear the RFI-L Condition

- 
- Step 1** Log into the node at the far-end node of the reporting ONS 15454.
  - Step 2** Check for alarms, especially LOS.

**Step 3** Resolve alarms in the far-end node.

---

## 1.5.114 RFI-P

- Not reported

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

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

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

### Procedure: Clear the RFI-P Condition

---

- Step 1** Verify that the ports are enabled and in-service on the reporting ONS 15454.
- Step 2** To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.
- Step 3** Look for alarms in the node with the failure, especially UNEQ-P or UNEQ-V.
- Step 4** Resolve alarms in that node.
- 

## 1.5.115 RFI-V

- Not reported

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

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



#### Caution

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

---

## Procedure: Clear the RFI-V Condition

- 
- Step 1** Check connectors to ensure they are securely fastened and connected to the correct slot/port.
  - Step 2** Verify that the DS1-14 port is active and in-service.
  - Step 3** Check the signal source for errors.
  - Step 4** Log into the node at the far-end of the reporting ONS 15454.
  - Step 5** Look for alarms in the far-end node, especially UNEQ-P or UNEQ-V.
  - Step 6** Find and troubleshoot the far-end node alarms.
- 

## 1.5.116 RING-MISMATCH

- Major, Service affecting

A Procedural Error Mismatch Ring alarm occurs when the Ring ID of the ONS 15454 that is reporting the alarm does not match the Ring ID of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical Ring IDs to function.

### Procedure: Clear the RING-MISMATCH Alarm

- 
- Step 1** Click the **Provisioning > Ring** tabs.
  - Step 2** Note the number in the Ring ID field.
  - Step 3** Log into the next ONS node in the BLSR.
  - Step 4** Verify that the Ring ID number matches the Ring ID number of the reporting node.
    - a. If the Ring ID matches the Ring ID in the reporting ONS node, log into the next ONS node in the BLSR.
    - b. If the Ring ID does not match the Ring ID in the reporting ONS node, change the Ring ID to match the Ring ID of the reporting node and click **Apply**.
    - c. Click **Yes** on the Accept Ring Map Changes dialog box.
    - d. Verify that the ring map is correct.
    - e. Click **Accept** for the new BLSR Ring Map.
  - Step 5** Repeat [Step 4](#) for all ONS nodes in the BLSR.
- 

## 1.5.117 SD-L

- Not Alarmed (NA) (Condition)

A signal degrade alarm occurs when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the signal degrade (SD) threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

The BER threshold on the ONS 15454 is user provisionable and has a range for SD from  $10^{-9}$  to  $10^{-5}$ . SD-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SD alarm travels on the B2 byte of the SONET overhead.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**


---

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

---

**Warning**


---

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

---

**Caution**


---

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

---

## Procedure: Clear the SD-L Condition

- 
- Step 1** Verify that the user-provisionable BER threshold is set at the expected level.
- a. From the CTC node view, double-click the card reporting the alarm to bring up the card view.
  - b. Click the **Provisioning > Line** tabs.
  - c. Under the SD BER column on the Provisioning pane, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.
  - d. If the entry is consistent with what the system was originally provisioned for, continue to [Step 2](#).
  - e. If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
  - f. Click **Apply**.
- Step 2** With an optical test set, measure the power level of the line to ensure it is within guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Clean the fibers at both ends for a line signal degrade:
- a. Clean the fiber according to local site practice.
  - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that single-mode fiber is used.
- Step 6** Verify that a single-mode laser is used at the far end.

- Step 7** If the problem persists, the transmitter at the other end of the optical line may be failing and require replacement.

**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 procedures.

## 1.5.118 SD-P

- Not Alarmed (NA) (Condition)

A signal degrade alarm occurs when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the signal degrade (SD) threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF. SD causes the card to switch from working to protect.

The BER threshold on the ONS 15454 is user provisionable and has a range for SD from  $10^{-9}$  to  $10^{-5}$ .

SD-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SD alarm travels on the B3 byte of the SONET overhead. The ONS 15454 detects path SD on the STS level, not the VT level.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**

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

**Warning**

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

**Caution**

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

### Procedure: Clear the SD-P Condition

- Step 1** Verify that the user-provisionable BER threshold is set at the expected level.
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.

- b. Click the **Provisioning > Line** tabs.
- c. Under the SD BER column on the Provisioning pane, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.
- d. If the entry is consistent with what the system was originally provisioned for, continue to step 2.
- e. If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
- f. Click **Apply**.

- Step 2** With an optical test set, measure the power level of the line to ensure it is within guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Verify that single-mode fiber is being used.
- Step 5** Verify that a single-mode laser is being used at the far end.
- Step 6** If the problem persists, the transmitter at the other end of the optical line may be failing and require replacement.

**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 procedures.

---

## 1.5.119 SF-L

- Not Alarmed (NA) (Condition)

A signal failure alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. Signal failure is defined by Telcordia as a “hard failure” condition. SD and SF both monitor the incoming BER error rate and are similar alarms, but SF is triggered at a higher BER than SD.

The BER threshold on the ONS 15454 is user provisionable and has a range for SF from  $10^{-5}$  to  $10^{-3}$ .

SF-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SF alarm travels on the B2 byte of the SONET overhead.

SF causes a card to switch from working to protect at either the path or line level. The SF alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**


---

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

---

**Warning**

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

**Caution**

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

## Procedure: Clear the SF-L Condition

- Step 1** Verify that the user-provisionable BER threshold is set at the expected level.
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.
  - Click the **Provisioning > Line** tabs.
  - Under the SF BER column on the Provisioning pane, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.
  - If the entry is consistent with what the system was originally provisioned for, continue to [Step 2](#).
  - If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
  - Click **Apply**.
- Step 2** Using an optical test set, measure the power level of the line and ensure it is within the guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Clean the fibers at both ends for a line signal fail:
- Clean the fiber according to local site practice.
  - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that single-mode fiber is being used.
- Step 6** Verify that a single-mode laser is being used at the far-end node.
- Step 7** If the problem persists, the transmitter at the other end of the optical line may be failing and need replacement.

**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 procedures.

## 1.5.120 SF-P

- Not Alarmed (NA) (Condition)

A signal failure alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. Signal failure is defined by Telcordia as a “hard failure” condition. SD and SF both monitor the incoming BER error rate and are similar alarms, but SF is triggered at a higher BER than SD.

The BER threshold on the ONS 15454 is user provisionable and has a range for SF from  $10^{-5}$  to  $10^{-3}$ .

SF-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SF alarm travels on the B3 byte of the SONET overhead. The ONS 15454 detects path SF on the STS level, not the VT level.

The SF alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.



**Warning**

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



**Warning**

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



**Caution**

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

### Procedure: Clear the SF-P Condition

- Step 1** Verify that the user-provisionable BER threshold is set at the expected level.
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.
  - Click the **Provisioning > Line** tabs.
  - Under the SF BER column on the Provisioning pane, verify that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.
  - If the entry is consistent with what the system was originally provisioned for, continue to step 2.
  - If the entry is not consistent with what the system was originally provisioned for, click on the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
  - Click **Apply**.
- Step 2** Using an optical test set, measure the power level of the line and ensure it is within the guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.



- Step 4** Verify that single-mode fiber is being used.
- Step 5** Verify that a single-mode laser is being used at the far-end node.
- Step 6** If the problem persists, the transmitter at the other end of the optical line may be failing and need replacement.

**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 procedures.

## 1.5.121 SFTWDOWN

- Minor, Non-service affecting

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

A software download in progress alarm occurs, when the TCC+ is downloading or transferring software. No action is necessary. Wait for the transfer or the software download to complete.

## 1.5.122 SFTWDOWN-FAIL

- Minor, Non-service affecting

The software download from the TCC+ card to the ONS 15454 has failed. The problem lies in the TCC+ card.

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC+ card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

### Procedure: Clear the SFTWDOWN-FAIL Alarm

- Step 1** Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.
- Step 2** If the download fails, reset the standby TCC+ to ensure that the standby card is synchronized with the database on the active TCC+:
- Identify the standby TCC+.
    - If you are looking at the physical ONS 15454, the ACT/STBY LED of standby TCC+ is amber.
    - If you are looking at the CTC node view of the ONS 15454, the standby TCC+ has a yellow LED depiction with the letters “Sby”.
  - Right-click on the standby TCC+.
  - Choose **Reset Card** from the pull-down menu.

- d. Click **Yes** at the Are You Sure dialog that appears.  
While the card resets, the FAIL LED will blink on the physical card and then no LED will be lit.  
While the card resets, the white LED with the letters “LDG” appears on the card in CTC.
- e. Verify that the reset is complete and error free.  
No new alarms appear under the Alarms tab on CTC.  
If you are looking at the physical ONS 15454, the ACT/STBY LED is lit.  
If you are looking at the CTC node view of the ONS 15454, a yellow LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.
- f. Wait ten minutes to verify that the Standby TCC+ does not reset itself.
- g. If the TCC+ reset is not complete and error free or if the TCC resets itself, call the Cisco Technical Assistance Center (1-800-553-2447).

- Step 3** Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.
- Step 4** If the software download fails again, refer to and complete the Back Up and Restore the Database procedure in the ONS 15454 Procedure Guide, then proceed to the next step in this procedure.
- Step 5** Reset the active TCC+:
- a. Identify the active TCC+.  
If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+ is green.  
If you are looking at the CTC node view of the ONS 15454, the active TCC+ has a green LED depiction with “Act”.
  - b. Right-click on the active TCC+.
  - c. Select **Reset Card** from the pull-down menu.
  - d. Click **Yes** at the Are You Sure dialog that appears.
  - e. Wait ten minutes to verify that the newly standby TCC+ does not reset itself.
  - f. Verify that the reset is complete and error free.  
No new alarms appear under the Alarms tab on CTC.  
If you are looking at the physical ONS 15454, the ACT/STBY LED has stopped blinking and is now amber.  
If you are looking at the CTC node view of the ONS 15454, a yellow LED depiction with Sby has replaced the blue/white depiction on the card in CTC. (The formerly active TCC+ is now standby.)
  - g. If the TCC+ reset is not complete and error free or if the TCC resets itself, call the Cisco Technical Assistance Center (1-800-553-2447).
- Step 6** Attempt the download again by clicking the **Maintenance > Software** tabs and the **Download** button.
- Step 7** If the download fails again, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- 

## 1.5.123 SNTP-HOST

- Minor, Non-service affecting

The SNTP (Simple Network Timing Protocol) host failure alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. This failure can result from two cause, either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

## Procedure: Clear the SNTP-HOST Alarm

- 
- Step 1** Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.
- Step 2** If the ping fails, contact the network administrator who manages the IP network supplying the SNTP information to the proxy and determine whether the network is experiencing problems which may affect the SNTP server/router connecting to the proxy ONS 15454.
- Step 3** Ensure that the ONS 15454 is provisioned correctly:
- On the ONS node serving as the proxy, click the CTC **Provisioning** > **General** tabs.
  - Ensure the **Enable Proxy** checkbox is checked.
  - If the **Enable Proxy** checkbox is not checked, check this box.
- Step 4** Refer to the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.
- 

## 1.5.124 SQUELCH

- Not Alarmed, Non-service affecting (Condition)

The ring is squelching traffic alarm occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance force ring commands. The isolation or failure of the node will disable the circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The AIS-P alarm will also appear on all nodes in the ring, except the isolated node.



**Caution**

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



**Warning**

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



**Warning**

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

## Procedure: Clear the SQUELCH Condition

- 
- Step 1** Determine the isolated node:
- a. Display the CTC network view.
  - b. The grayed out node with red spans will be the isolated node.
- Step 2** Verify fiber continuity to the ports on the isolated node.
- Step 3** Verify that the proper ports are in service.
- Step 4** Use an optical test set to verify that a valid signal exists on the line.  
Test the line as close to the receiving card as possible.
- Step 5** Verify that the power level of the optical signal is within the optical card's receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.
- Step 6** Ensure that the optical transmits and receives are connected properly.
- Step 7** 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 procedures.

---

## 1.5.125 SSM-FAIL

- Minor, Non-service affecting

The Failed to Receive Synchronization Status Message alarm occurs when the synchronization status messaging (SSM) received by the ONS 15454 fails. The problem is external to ONS 15454. The ONS 15454 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

SSM is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET line layer. They enable SONET devices to automatically select the highest quality timing reference and to avoid timing loops.

## Procedure: Clear the SSM-FAIL Alarm

- 
- Step 1** Verify that SSM is enabled on the external timing source.
- Step 2** Use a test set to determine that the external timing source is delivering SSM.
- 

## 1.5.126 SSM-STU

- Not Alarmed (NA) (Condition)

The Synchronization Traceability Unknown alarm occurs when the reporting node is timed to a reference that does not support synchronization status messaging (SSM), but the ONS 15454 has SSM support enabled. STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

SSM is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET line layer. SSM enables SONET devices to automatically choose the highest quality timing reference and to avoid timing loops.

## Procedure: Clear the STU Condition

- 
- Step 1** Click the **Provisioning > Timing** tabs.
- Step 2** If **Sync Messaging** is checked, uncheck the box.
- Step 3** If **Sync Messaging** is unchecked, check the box.
- Step 4** Click **Apply**.
- 

## 1.5.127 SWMTXMOD

- Critical, Service affecting

The Switching Matrix Module Failure alarm occurs on the XCVT card or a traffic card. If the alarm reports against a traffic card, it means that the logic component on the cross-connect card is out of frame (OOF) with the logic component on the reporting traffic card. All traffic on the reporting traffic card is lost.

If the alarm reports against an XCVT card, it means that a logic component internal to the reporting XCVT card is out of frame with a second logic component on the same XCVT card. One or more traffic cards may lose traffic as a result of this failure.

## Procedure: Clear the SWMTXMOD Alarm

- 
- Step 1** If the card reporting the alarm is the standby XCVT card, perform a CTC reset on the standby XCVT:
- Display the node view.
  - Position the cursor over the slot reporting the alarm.
  - Right-click and choose **RESET CARD**.
  - Click **Yes** at the **Resetting Card** confirmation dialog.  
Wait for the card to reboot.
  - If the alarm persists, physically reseal the standby XCVT card.
- Step 2** If the card reporting the alarm is the active XCVT card, perform a side switch from the active XCVT card to the standby XCVT card:
- Determine the active XCVT card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.




---

**Note** You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

---

- b. In the node view, choose the **Maintenance > XC Cards** tabs.
- c. Click **Switch**.
- d. Click **Yes** on the Confirm Switch dialog box.




---

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

---

- e. Perform a CTC reset on the reporting card:
  - From the node view, position the cursor over the slot reporting the alarm.
  - Right-click to choose **RESET CARD**.
  - Click **Yes** at the **Resetting Card** confirmation dialog.
  - Wait for the card to reboot.
- f. If the alarm persists, physically reseal the standby XCVT card.

**Step 3** If the card reporting the alarm is an I/O card, perform a side switch from the active cross-connect (XC, XCVT, XC10G) card to the standby cross-connect card:

- a. Determine the active cross-connect (XC, XCVT, XC10G) card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.




---

**Note** You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

---

- b. In the node view, choose the **Maintenance > XC Cards** tabs.
  - c. Click **Switch**.
  - d. Click **Yes** on the Confirm Switch dialog box. After the active card goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.
  - e. If the alarm does not clear after the cross-connect (XC, XCVT, XC10G) side switch, perform a CTC reset on the reporting card:
  - f. Display the CTC node view.
  - g. Position the cursor over the slot reporting the alarm.
  - h. Right-click to choose **RESET CARD**.
  - i. Click **Yes** at the **Resetting Card** confirmation dialog.
    - Wait for the card to reboot.
  - j. If the alarm persists, physically reseal the reporting traffic/line card.
-

## 1.5.128 SWTOPRI

- Not Alarmed (NA) (Condition)

The synchronization switch to primary reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.



**Note**

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

## 1.5.129 SWTOSEC

- Not Alarmed (NA) (Condition)

The synchronization switch to secondary reference condition occurs when the ONS 15454 has switched to the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

To clear the SWTOSEC condition, find and troubleshoot alarms related to failures of the primary source, such as the SYNCPRI alarm.

## 1.5.130 SWTOHIRD

- Not Alarmed (NA) (Condition)

The synchronization switch to third reference condition occurs when the ONS 15454 has switched to the third timing source (reference 3). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

To clear the SWTOHIRD condition, find and troubleshoot alarms related to failures of the primary and secondary reference source, such as the SYNCPRI and SYNCSEC alarms.

## 1.5.131 SYNCPRI

- Minor, Non-service affecting

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). This switch also triggers the SWTOSEC alarm.

### Procedure: Clear the SYNCPRI Condition

- 
- Step 1** From the node view, click the **Provisioning > Timing** tabs.
- Step 2** Check the current configuration for the REF-1 of the NE Reference.
- Step 3** If the primary reference is a BITS input, follow the procedure in the [“LOS \(BITS\)” section on page 1-66](#).

- Step 4** If the primary reference clock is an incoming port on the ONS 15454, follow the procedure in the “[LOS \(OC-N\)](#)” section on page 1-68.
- 

## 1.5.132 SYNCSEC

- Minor, Non-service affecting

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. This switch also triggers the SWTOTHIRD condition.

### Procedure: Clear the SYNCSEC Alarm

---

- Step 1** From the node view, click the **Provisioning > Timing** tabs.
- Step 2** Check the current configuration of the REF-2 for the NE Reference.
- Step 3** If the secondary reference is a BITS input, follow the procedure in the “[LOS \(BITS\)](#)” section on page 1-66.
- Step 4** If the secondary timing source is an incoming port on the ONS 15454, follow the procedure in the “[LOS \(OC-N\)](#)” section on page 1-68.
- 

## 1.5.133 SYNCTHIRD

- Minor, Non-service affecting

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC+ card may have failed. The ONS 15454 often reports either FRNGSYNC or HLDOVERSYNC alarms after a SYNCTHIRD alarm.



#### Caution

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

---

### Procedure: Clear the SYNCTHIRD Alarm

---

- Step 1** From node view, click the **Provisioning > Timing** tabs.
- Step 2** Check the current configuration of the REF-3 for the NE Reference.
- Step 3** If the third timing source is a BITS input, follow the procedure in the “[LOS \(BITS\)](#)” section on page 1-66.



- Step 4** If the third timing source is an incoming port on the ONS 15454, follow the procedure in the [“LOS \(OC-N\)” section on page 1-68](#).
- Step 5** If the third timing source uses the internal ONS 15454 timing, perform a CTC reset on the TCC+ card:
- In node view, run the mouse over the TCC+ card and a pop up box will display if the card is active or standby.
  - Position the cursor over the active TCC+ card slot.
  - Right-click and choose **RESET CARD**.
  - Click **Yes** when the “Are You Sure?” dialog box appears.
  - Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
  - Confirm that the TCC+ you reset is in standby mode after the reset:  
The TCC+ card’s LED will be amber for standby or green for active, or  
In node view, run the mouse over the TCC+ card and a pop up box will display whether the card is active or standby.
- Step 6** If this fails to clear the alarm, physically reseat the TCC+ card. See the [“Reset the TCC+ With a Card Pull” section on page 3-5](#).
- Step 7** If the reset fails to clear the alarm, replace the TCC+ card.

**Note**

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

## 1.5.134 SYSBOOT

- Major, Service affecting

The System Reboot alarm indicates that new software is booting on the TCC+ card. This is an informational alarm. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

## 1.5.135 TIM-P

- Minor, Service affecting

The STS Path Trace Identifier Mismatch Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to manual or Auto for this alarm to occur.

In manual mode at the Path Trace screen, the user types the expected string into the New Expected String field for the receiving port. This string must match the string typed into the New Transmit String field for the sending port. If these fields do not match, the TIM-P alarm will occur. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, this means the circuit path changed or someone entered a new incorrect value into the New Transmit String field. Follow the procedure below to clear either instance.

TIM-P also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. This TIM-P occurrence is usually accompanied by other alarms, such as LOS, UNEQ-P, or PLM-P. In this case, reattach or replace the original cables/fibers to clear the alarm.

## Procedure: Clear the TIM-P Alarm

- 
- Step 1** Log into the circuit source node and select the **Circuits** tab.
  - Step 2** Select the circuit reporting the alarm, then click **Edit**.
  - Step 3** At the bottom of the Edit Circuit window, check the **Show Detailed Map** box.
  - Step 4** On the detailed circuit map, right-click the source circuit port and choose **Edit Path Trace** from the shortcut menu.
  - Step 5** On the detailed circuit map, right-click the drop/destination circuit port and choose **Edit Path Trace** from the shortcut menu.
  - Step 6** Compare the New Transmit String and the New Expected String entries in the Path Trace Mode dialog box.
  - Step 7** If the strings differ, correct the Transmit or Expected strings and click **Apply**.
  - Step 8** Click **Close**.
- 

## 1.5.136 TPTFAIL

- Major, Service affecting

The transport layer failure alarm indicates a break in the end-to-end Ethernet link integrity feature of the G1000-4 cards. This alarm indicates a far-end condition and not a problem with the port reporting TPTFAIL.

This alarm indicates a problem on either the SONET path or the remote Ethernet port, which prevents the complete end-to-end Ethernet path from working. If there is any SONET path alarm such as AIS-P, LOP-P, UNEQ-P, PDI-P, or RDI-P on the SONET path used by the Ethernet port, the affected port raises a TPTFAIL alarm. Also, if the far-end G1000-4 Ethernet port is administratively disabled or it is seeing a CARLOSS condition it will set the C2 byte in the SONET path overhead to indicate a payload defect condition (PDI-P) which in turn will cause a TPTFAIL to be reported against this near-end port.

With a TPTFAIL condition, the near-end port is automatically disabled (transmit laser turned off) when this condition occurs. In turn this can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter and also cause a CARLOSS condition to occur on this port. In all cases the source problem is either in the SONET path being used by this G1000-4 port or the far-end G1000-4 port to which it is mapped.

## Procedure: Clear the TPTFAIL Alarm

- 
- Step 1** An occurrence of TPTFAIL on a G1000-4 port indicates either a problem with the SONET path that this port is using or with the far end G1000-4 port that is mapped to this port. Lookup and troubleshoot any alarms being reported by the OC-N card utilized by the Ethernet circuit of the G1000-4.

- Step 2** If no alarms are reported by the OC-N card or a PDI-P condition is reported the problem may be on the far-end G1000-4 port that the port reporting TPTFAIL is mapped to. Lookup and troubleshoot any alarms, such as CARLOSS, reported against the far-end port or card.
- 

## 1.5.137 TRMT

- Major, Service affecting

A facility termination equipment transmit failure alarm occurs when there is a transmit failure on the DS1-14 card because of an internal hardware failure. The card must be replaced.

### Procedure: Clear the TRMT Alarm

- Step 1** Replace the DS1-14 card reporting the failure.



**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 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 2** Call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).
- 

## 1.5.138 TRMT-MISS

- Major, Service affecting

A facility termination equipment transmitter missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. This means transmit cable is missing on the DS1-14 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector connects to a DS1-14 card instead of a DS-3 card.



**Note**

DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

---

### Procedure: Clear the TRMT-MISS Alarm

- Step 1** Check that the device attached to the DS1-14 port is operational.
- Step 2** Verify that the cabling is securely connected.
- Step 3** Verify that the pinouts are correct.

**Step 4** If Steps 1 – 3 do not clear the alarm, replace the transmit cable.

---

## 1.5.139 UNEQ-P

- Critical, Service affecting

A Signal Label Mismatch Failure Unequipped Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

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

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



### Note

If you have created a new circuit but it has no signal, an UNEQ-P alarm is reported on the OC-N cards and an AIS-P alarm is reported on the terminating cards. These alarms clear when the circuit carries a signal.

---



### Caution

Deleting a circuit affects traffic.

---



### Caution

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

---

## Procedure: Clear the UNEQ-P Alarm

---

- Step 1** Display the CTC network view and right-click the span reporting UNEQ-P.
- Step 2** Select **Circuits** from the menu.
- Step 3** If the specified circuit is a VT tunnel, check for VTs assigned to the VT tunnel.
- Step 4** If the VT tunnel has no assigned VTs, delete the VT tunnel from the list of circuits.
- Step 5** If you have complete visibility to all nodes, check for incomplete circuits such as stranded bandwidth from circuits that were not deleted completely.
- Step 6** If you find incomplete circuits, verify whether they are working circuits and if they are continue to pass traffic.
- Step 7** If the incomplete circuits are not needed or are not passing traffic, delete them and log out of CTC. Log back in and check for incomplete circuits again. Recreate any needed circuits.
- Step 8** Verify that all circuits terminating in the reporting card are active:
  - a. Click the **Circuits** tab.

- b. Verify that the State column lists the port as ACTIVE.
  - c. If the State column lists the port as INCOMPLETE. If INCOMPLETE does not change after a full initialization, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- Step 9** After you determine that the port is active, verify the signal source received by the card reporting the alarm.
- Step 10** Check the far-end OC-N card that provides STS payload to the card.
- Step 11** Verify the far-end cross-connect between the OC-N card and the DS-N card.
- Step 12** Clean the far-end optical fiber:
- a. Clean the fiber according to local site practice.
  - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.



Warning

---

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

---



Warning

---

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

---

## 1.5.140 UNEQ-V

- Major, Service affecting

An signal label mismatch failure unequipped path alarm indicates that the node is receiving SONET path overhead with bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is the node that is transmitting the VT-level signal into the node reporting the UNEQ-P. The problem node is the next node upstream that processes the signal at the VT level.

The V in UNEQ-V indicates that the failure has occurred at the VT layer. The VT (electrical) layer is created when the SONET signal is broken down into an electrical signal, for example, when an optical signal comes into an ONS 15454, the optical signal is demultiplexed and one of the channels separated from the optical signal is cross connected into an ONS 15454 cross-connect (XC/XCVT/XC10G) card and the corresponding DS-N card.



Warning

---

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

---

**Warning**

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

**Caution**

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

## Procedure: Clear the UNEQ-V Alarm

- Step 1** Verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
  - Verify that the State column lists the port as ACTIVE.
  - If the State column lists the port as INCOMPLETE. If INCOMPLETE does not change after full initialization, log on to <http://www.cisco.com/tac> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

**Step 2** After you determine that the port is active, verify the signal source being received by the DS-N card reporting the alarm.

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



**Caution** Deleting a circuit can be service affecting.

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

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

**Step 6** Clean the far-end optical fiber:

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

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

**Caution**

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



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

## 1.6 DS3-12E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M23, or C-bit. The choice of framing format affects which line alarms the DS3-12E card reports. The table below lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms as the standard DS-3 card.

**Table 1-4 DS3-12E Line Alarms**

Alarm	UNFRAMED	M23	CBIT
LOS	◆	◆	◆
AIS	◆	◆	◆
LOF	○	◆	◆
IDLE	○	◆	◆
RAI	○	◆	◆
Terminal Lpbk	◆	◆	◆
Facility Lpbk	◆	◆	◆
FE Lpbk	○	○	◆
FE Common Equipment Failure	○	○	◆
FE Equipment Failure-SA	○	○	◆
FE LOS	○	○	◆
FE LOF	○	○	◆
FE AIS	○	○	◆
FE IDLE	○	○	◆
FE Equipment Failure-NSA	○	○	◆







## General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454. To troubleshoot specific ONS 15454 alarms, see [Chapter 1, “Alarm Troubleshooting.”](#) If you cannot find what you are looking for in this chapter or [Chapter 1, “Alarm Troubleshooting,”](#) contact the Cisco Technical Assistance Center (TAC) at 1-877-323-7368.

This chapter begins with the following sections on network problems:

- [Network Troubleshooting Tests](#)—Describes loopbacks and hairpin circuits, which you can use to test circuit paths through the network or logically isolate faults.



### Note

---

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

---

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

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

- [CTC Operation and Connectivity](#)—Provides troubleshooting procedures for CTC log-in or operation errors and PC and network connectivity.
- [Circuits and Timing](#)—Provides troubleshooting procedures for circuit creation, and error reporting, and timing reference errors and alarms.
- [Fiber and Cabling](#)—Provides troubleshooting procedures for fiber and cabling connectivity errors.

## 2.1 Network Troubleshooting Tests

Use loopbacks and hairpins to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 line (traffic) cards, except Ethernet cards, allow loopbacks and hairpins.



### Caution

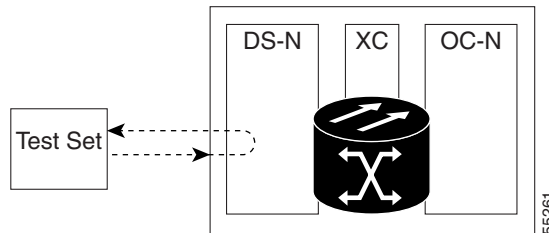
---

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

---

A facility loopback tests the line interface unit (LIU) of a card, the EIA (electrical interface assembly), and related cabling. After applying a facility loopback on a card, use a test set to run traffic over the loopback. A successful facility loopback eliminates the LIU, the EIA, or cabling plant as the potential cause of a network problem. [Figure 2-1](#) shows a facility loopback on a DS-N card.

**Figure 2-1** The facility loopback process on a DS-N card



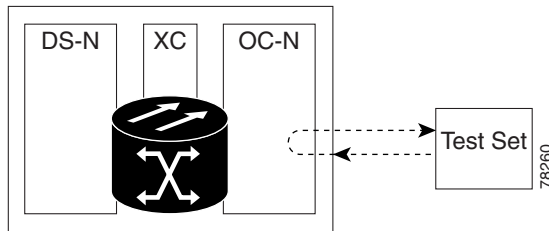
[Figure 2-2](#) shows a facility loopback on an OC-N card.



**Caution**

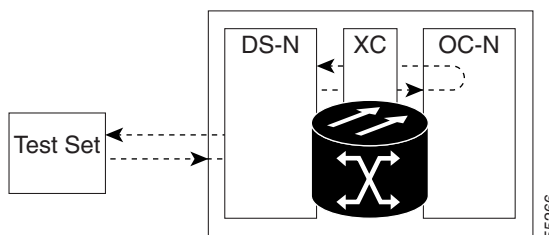
Before performing a facility loopback on an OC-N card, make sure the card contains at least two SDCC paths to the node where the card is installed. A second SDCC path provides a non-looped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second SDCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N card.

**Figure 2-2** The facility loopback process on an OC-N card



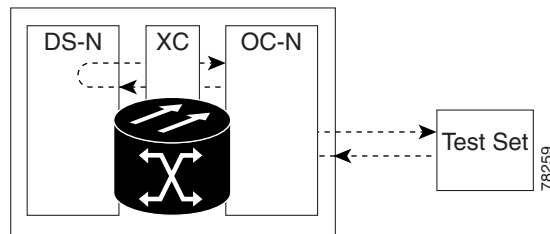
A terminal loopback tests a circuit path as it passes through the cross-connect card (XC, XCVT, or XC10G) and as it loops back from the card being tested. [Figure 2-3](#) shows a terminal loopback on an OC-N card. The test-set traffic comes in on the DS-N card and goes through the cross-connect card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it through the cross-connect card to the DS-N card. This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the OC-N card.

**Figure 2-3** The terminal loopback process on an OC-N card



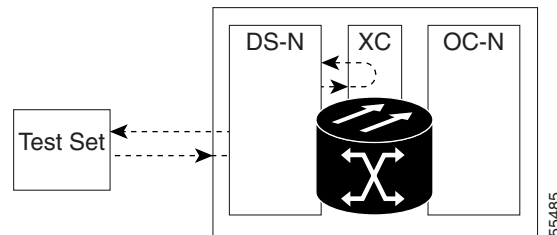
To test the LIU on an OC-N card, connect an optical test set to the OC-N card ports and perform a facility loopback or use a loopback or hairpin on a card that is farther along the circuit path. Figure 2-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it through the cross-connect card to the OC-N card. This test verifies that the cross-connect card and circuit paths are valid, but does not test the LIU on the DS-N card.

**Figure 2-4** The terminal loopback process on a DS-N card



A hairpin circuit brings traffic in and out on a DS-N port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, thus preventing a drop of all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic.

**Figure 2-5** The hairpin circuit process on an OC-N card



## 2.2 Identify Points of Failure on a Circuit Path

Facility loopbacks, terminal loopbacks, and hairpin circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a network test at each point along the circuit path systematically eliminates possible points of failure. The example in this section tests a DS-N circuit on a two-node bidirectional line switched ring (BLSR). Using a series of facility loopbacks, terminal loopbacks, and hairpins, the path of the circuit is traced and the possible points of failure eliminated.

A logical progression of four network test procedures apply to this scenario:



**Note**

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

1. A facility loopback on the source-node DS-N card
2. A hairpin on the source-node DS-N card
3. A terminal loopback on the destination-node DS-N card

4. A facility loopback on the destination DS-N card

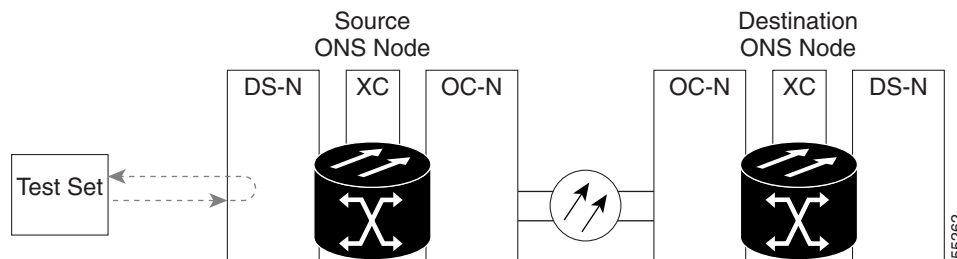
**Note**

All loopback tests require on-site personnel.

## 2.2.1 Perform a Facility Loopback on a Source DS-N Card

The facility loopback test is performed on the source card in the network circuit, in this example, the DS-N card in the source node. Completing a successful facility loopback on this card eliminates the cabling, the DS-N card, and the EIA as possible failure points. Figure 2-6 shows an example of a facility loopback on a source DS-N card.

**Figure 2-6** A facility loopback on a circuit source DS-N card

**Caution**

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

### 2.2.1.1 Create the Facility Loopback on the Source DS-N Card

- Step 1** Connect an electrical test set to the port you are testing.
- Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The transmit (Tx) and receive (Rx) terminals connect to the same port. Adjust the test set accordingly.
- Step 2** Use CTC to create the facility loopback circuit on the port being tested:
- a. In node view, double-click the card where you will perform the loopback.
  - b. Click the **Maintenance > Loopback** tabs.
  - c. Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.
  - d. Click **Apply**.
  - e. On the confirmation dialog box, click **Yes**.

**Note**

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

**Step 3** Proceed to the [“Test the Facility Loopback Circuit”](#) section on page 2-5.

---

### 2.2.1.2 Test the Facility Loopback Circuit

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the facility loopback.
- Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Hairpin on a Source Node”](#) section on page 2-7.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.
- Step 5** Proceed to the [“Test the DS-N Cabling”](#) section on page 2-5.
- 

### 2.2.1.3 Test the DS-N Cabling

- Step 1** Replace the suspect cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.
- Step 2** If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the DSx panel or the EIA and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.
- Step 3** Resend test traffic on the loopback circuit with a known-good cable installed.
- Step 4** If the test set indicates a good circuit, the problem was probably the defective cable.
- Replace the defective cable.
  - Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Hairpin on a Source Node”](#) section on page 2-7.
- Step 5** If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty EIA.
- Step 6** Proceed to the [“Test the DS-N Card”](#) section on page 2-5.
- 

### 2.2.1.4 Test the DS-N Card

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



**Caution**

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

---

**Identify Points of Failure on a Circuit Path**

- Step 2** Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
- Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
  - Replace the faulty card.
  - Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Hairpin on a Source Node” section on page 2-7](#).
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty EIA.
- Step 5** Proceed to the [“Test the EIA” section on page 2-6](#).
- 

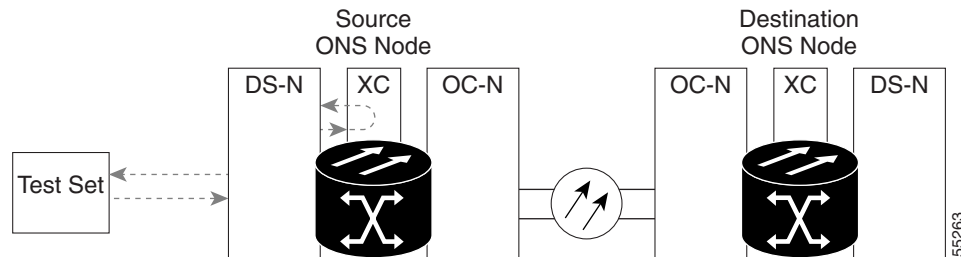
## 2.2.1.5 Test the EIA

- 
- Step 1** Remove and reinstall the EIA to ensure a proper seating:
- Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
  - Loosen the nine perimeter screws that hold the EIA panel in place.
  - Lift the EIA panel by the bottom to remove it from the shelf assembly.
  - Follow the installation procedure for the appropriate EIA. See the [“Replace the Electrical Interface Assembly” section on page 3-20](#).
- Step 2** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA.
- Step 3** If the test set indicates a good circuit, the problem was probably an improperly seated EIA.
- Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Hairpin on a Source Node” section on page 2-7](#)
- Step 4** If the test set indicates a faulty circuit, the problem is probably the defective EIA.
- Return the defective EIA to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.
  - Replace the faulty EIA.
- Step 5** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.
- Step 6** If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.
- Step 7** If the test set indicates a good circuit, the problem was probably the defective EIA.
- Clear the loopback circuit before testing the next segment of the circuit path.
  - Proceed to the [“Perform a Hairpin on a Source Node” section on page 2-7](#).
-

## 2.2.2 Perform a Hairpin on a Source Node

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card eliminates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 2-7 shows an example of a hairpin loopback on a source node.

Figure 2-7 Hairpin on a source node



**Note**

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

### 2.2.2.1 Create the Hairpin on the Source Node

- Step 1** Connect an electrical test set to the port you are testing.
- If you just completed the “[Perform a Facility Loopback on a Source DS-N Card](#)” section on page 2-4, leave the electrical test set hooked up to the DS-N card in the source node.
  - If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The transmit (Tx) and receive (Rx) terminals connect to the same port.
  - Adjust the test set accordingly.
- Step 2** Use CTC to set up the hairpin on the port being tested:
- Click the **Circuits** tab and click the **Create** button.
  - Give the circuit an easily identifiable name, such as hairpin1.
  - Set the Circuit **Type** and **Size** to the normal preferences.
  - Uncheck the **Bidirectional** checkbox and click **Next**.
  - In the Circuit Source dialog box, fill in the same card and port where the facility loopback test (DS-N card in the source node) was performed and click **Next**.
  - In the Circuit Destination dialog box, use the same card and port used for the Circuit Source dialog box and click **Finish**.
- Step 3** Confirm that the newly created circuit appears with a direction column indicating that this circuit is one-way.

**Step 4** Proceed to the [“Test the Hairpin Circuit”](#) section on page 2-8

---

## 2.2.2.2 Test the Hairpin Circuit

- 
- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit.
- Clear the hairpin circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Card”](#) section on page 2-9.
- Step 4** If the test set indicates a faulty circuit, there may be a problem with the cross-connect card.
- Step 5** Proceed to the [“Test the Standby Cross-Connect Card”](#) section on page 2-8.
- 

## 2.2.2.3 Test the Standby Cross-Connect Card

- 
- Step 1** Perform a reset on the standby cross-connect card:
- Determine the standby cross-connect card. On both the physical node and the CTC screen, the ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
  - Position the cursor over the standby cross-connect card.
  - Right-click and choose **RESET CARD**.
- Step 2** Do a manual switch (side switch) of the cross-connect cards before retesting the loopback circuit:



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

---

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



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

---

- Step 3** Resend test traffic on the loopback circuit.
- The test traffic now travels through the alternate cross-connect card.



- Step 4** If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem.
- Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Card”](#) section on page 2-9.
- Step 5** If the test set indicates a good circuit, the problem may be a defective card.
- Step 6** To confirm a defective original cross-connect card, proceed to the [“Retest the Original Cross-Connect Card”](#) section on page 2-9.
- 

### 2.2.2.4 Retest the Original Cross-Connect Card

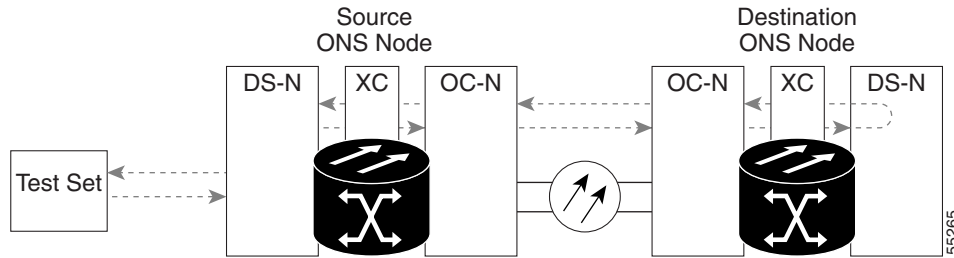
---

- Step 1** Do a manual switch (side switch) of the cross-connect cards to make the original cross-connect card the active card.
- Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
  - In node view, select the **Maintenance > XC Cards** tabs.
  - From the Cross Connect Cards menu, choose **Switch**.
  - Click **Yes** on the Confirm Switch dialog box.
- Step 2** Resend test traffic on the loopback circuit.
- Step 3** If the test set indicates a faulty circuit, the problem is probably the defective card.
- Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case
  - Replace the defective cross-connect card. See [Chapter 1, “Alarm Troubleshooting”](#) for details.
  - Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Card”](#) section on page 2-9
- Step 4** If the test set indicates a good circuit, the cross-connect card may have had a temporary problem that was cleared by the side switch.
- Clear the loopback circuit before testing the next segment of the network circuit path.
  - Proceed to the [“Perform a Terminal Loopback on a Destination DS-N Card”](#) section on page 2-9.
- 

### 2.2.3 Perform a Terminal Loopback on a Destination DS-N Card


This test is a terminal loopback performed on the destination line card in the circuit, in the following example the DS-N card in the destination node. First, create a bidirectional circuit that starts on the source node DS-N port and terminates on the destination node DS-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a destination node DS-N card verifies that the circuit is good up to the destination DS-N. [Figure 2-8](#) shows an example of a terminal loopback on a destination DS-N card.

Figure 2-8 Terminal loopback on a destination DS-N card

**Caution**

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

### 2.2.3.1 Create the Terminal Loopback on a Destination DS-N Card

- Step 1** Connect an electrical test set to the port you are testing:
- If you just completed the [“Perform a Hairpin on a Source Node”](#) section on page 2-7, leave the electrical test set hooked up to the DS-N card in the source node.
  - If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.
  - Adjust the test set accordingly.
- Step 2** Use CTC to set up the terminal loopback circuit on the port being tested.
- Click the **Circuits** tab and click the **Create** button.
  - Give the circuit an easily identifiable name, such as “DSNtoDSN”.
  - Set Circuit **Type** and **Size** to the normal preferences.
  - Leave the **Bidirectional** checkbox checked and click **Next**.
  - In the Circuit Source dialog box, fill in the same card and port where the facility loopback test (the DS-N card in the source node) was performed and click **Next**.
  - In the Circuit Destination dialog box, fill in the destination card and port (the DS-N card in the destination node) and click **Finish**.
- Step 3** Confirm that the newly created circuit appears on a Circuits screen row with a direction column that shows a two-way circuit.
-  **Note** It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.
- Step 4** Create the loopback circuit on the destination card and port being tested:
- In node view, double-click the card that requires the loopback, such as the DS-N card in the destination node.
  - Click the **Maintenance > Loopback** tabs.

- c. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.
  - d. Click **Apply**.
  - e. On the confirmation dialog box, click **Yes**.
- Step 5** Proceed to the [“Test the Terminal Loopback Circuit on the Destination DS-N Card”](#) section on page 2-11.
- 

### 2.2.3.2 Test the Terminal Loopback Circuit on the Destination DS-N Card

---

- Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Proceed to the [“Perform a Facility Loopback on a Destination DS-N Card”](#) section on page 2-11.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty card. Proceed to the [“Test the Destination DS-N Card”](#) section on page 2-11.
- 

### 2.2.3.3 Test the Destination DS-N Card

---

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



**Caution**

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

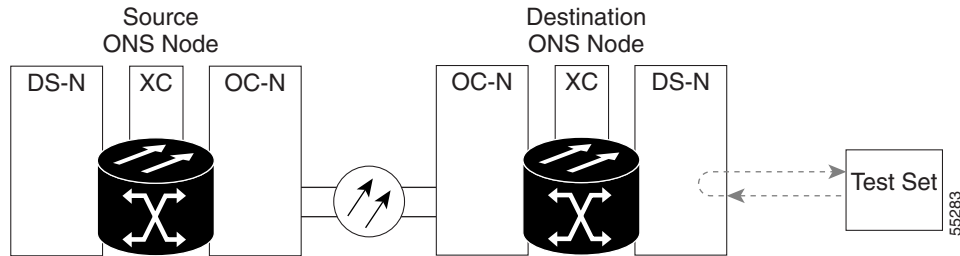
---

- Step 2** Resend test traffic on the loopback circuit with a known-good card.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
- a. Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.
  - b. Replace the defective DS-N card.
- Step 4** Proceed to the [“Perform a Facility Loopback on a Destination DS-N Card”](#) section on page 2-11.
- 

## 2.2.4 Perform a Facility Loopback on a Destination DS-N Card

The final test is a facility loopback performed on the last card in the circuit, in this case the DS-N card in the destination node. Completing a successful facility loopback on this card eliminates the possibility that the destination node cabling, DS-N card, LIU, or EIA is responsible for a faulty circuit. [Figure 2-9](#) shows an example of a facility loopback on a destination DS-N card.

Figure 2-9 Facility loopback on a destination DS-N card

**Caution**

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

### 2.2.4.1 Create a Facility Loopback Circuit on a Destination DS-N Card

- Step 1** Connect an electrical test set to the port you are testing:
- Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the EIA connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Set up your test set accordingly.
- Step 2** Use CTC to create the facility loopback circuit on the port being tested:
- In node view, double-click the card where the loopback will be performed.
  - Click the **Maintenance > Loopback** tabs.
  - Select **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the row appropriate for the desired port.
  - Click **Apply**.
  - On the confirmation dialog box, click **Yes**.

**Note**

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

- Step 3** Proceed to the “[Test the Facility Loopback Circuit](#)” section on page 2-12.

### 2.2.4.2 Test the Facility Loopback Circuit

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

- b. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.
- Step 5** Proceed to the [“Test the DS-N Cabling”](#) section on page 2-5.
- 

### 2.2.4.3 Test the DS-N Cabling

- Step 1** Replace the suspect cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable.
- Step 2** If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the DSx panel or the EIA and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.
- Step 3** Resend test set traffic on the loopback circuit with a known-good cable installed.
- Step 4** If the test set indicates a good circuit, the problem was probably the defective cable.
- a. Replace the defective cable.
  - b. Clear the loopback circuit.
  - c. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 5** If the test set indicates a faulty circuit, the problem may be a faulty card or a faulty EIA.
- Step 6** Proceed to the [“Test the DS-N Card”](#) section on page 2-5.
- 

### 2.2.4.4 Test the DS-N Card

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

**Caution**

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

---

- Step 2** Resend test traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
- a. Return the defective card to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.
  - b. Replace the faulty card. See [Chapter 1, “Alarm Troubleshooting”](#) for details.
  - c. Clear the loopback circuit.
  - d. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty EIA.

**Step 5** Proceed to the “[Test the EIA](#)” section on page 2-6.

---

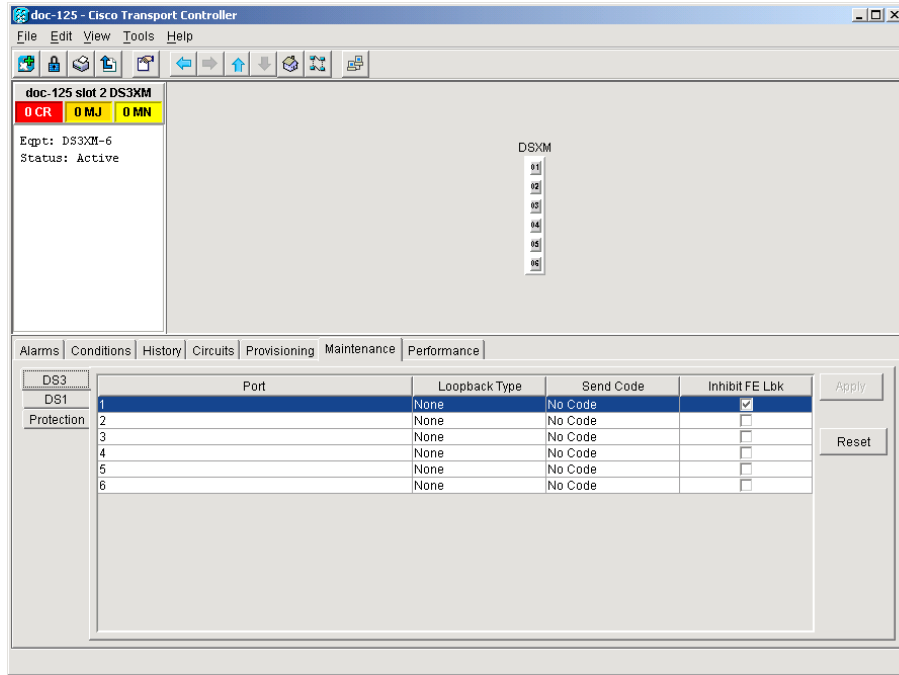
### 2.2.4.5 Test the EIA

- 
- Step 1** Remove and reinstall the EIA to ensure a proper seating.
- a. Remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454, and pull it away from the shelf assembly.
  - b. Loosen the nine perimeter screws that hold the EIA panel in place.
  - c. Lift the EIA panel by the bottom to remove it from the shelf assembly.
  - d. Follow the installation procedure for the appropriate EIA. See the “[Replace the Electrical Interface Assembly](#)” section on page 3-20.
- Step 2** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA.
- Step 3** If the test set indicates a good circuit, the problem was probably an improperly seated EIA.
- a. Clear the loopback circuit.
  - b. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 4** If the test set indicates a faulty circuit, the problem is probably the defective EIA.
- a. Return the defective EIA to Cisco through the RMA process. Call the Cisco TAC at 1-877-323-7368 to open an RMA case.
  - b. Replace the faulty EIA.
- Step 5** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.
- Step 6** If the test set indicates a faulty circuit, repeat all of the facility loopback procedures. If the faulty circuit persists, call Cisco TAC at 1-877-323-7368 for assistance.
- Step 7** If the test set indicates a good circuit, the problem was probably the defective EIA.
- a. Clear the loopback circuit.
  - b. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- 

## 2.2.5 Using the DS3XM-6 Card FEAC (Loopback) Functions

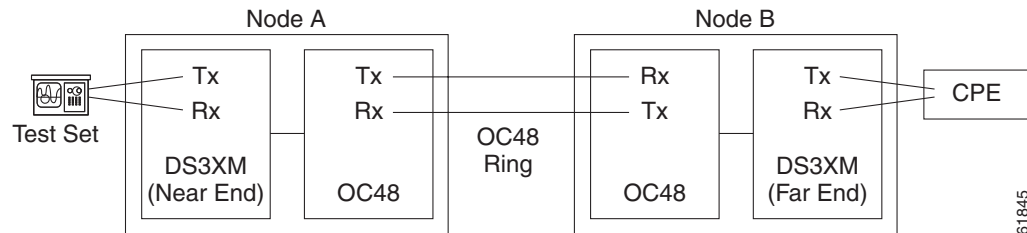
The DS3XM-6 card supports Far End Alarm and Control (FEAC) features that are not available on basic DS-3 cards. Click the Maintenance tab at the DS3XM-6 card view to reveal the two additional DS3XM-6 columns. [Figure 2-10](#) shows the DS3 subtab and the additional *Send Code* and *Inhibit FE Lbk* columns.

Figure 2-10 Accessing FEAC functions on the DS3XM-6 card



The far end in FEAC refers to the piece of equipment that is connected to the DS3XM-6 card and not the far end of a circuit. In Figure 2-11, if a DS3XM-6 (near-end) port is configured to send a Line Loop Code, the code will be sent to the connected test set, not the DS3XM-6 (far-end) port.

Figure 2-11 Diagram of far end action code



### 2.2.5.1 FEAC Send Code

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

## 2.2.5.2 FEAC Inhibit Loopback

The DS3XM-6 ports and transmuted DS-1s initiate loopbacks when they receive FEAC Line Loop codes. If the Inhibit Loopback checkbox is checked for a DS-3 port, then that port will ignore any received FEAC Line Loop codes and will not loop back. The port can still be put into loopback manually using the Loopback Type column even if the Inhibit Loopback box is selected. Only DS-3 ports can be configured to inhibit responses to FEAC loopback commands, individual DS-1 ports cannot inhibit their responses.

## 2.2.5.3 FEAC Alarms

The node raises a LPBKDS3FEAC-CMD or LPBKDS1FEAC-CMD alarm for a DS-1 or DS-3 port if a FEAC loopback code is sent to the far end.

If the ONS 15454 port is in loopback from having received a loopback activate FEAC code, a LPBKDS3FEAC or LPBKDS1FEAC alarm occurs. The alarm will clear when a loopback deactivate FEAC command is received on that port.

A DS3E card will respond to, and can inhibit, received FEAC DS3 level loopback codes. A DS3E card cannot be configured to send FEAC codes.

# 2.3 CTC Operation and Connectivity

This section contains troubleshooting procedures for CTC login or operation errors and PC and network connectivity.

## 2.3.1 Operation: Unable to Change Node View to Network View

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

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

**Table 2-1 Browser Stalls When Downloading Files From TCC+**

Possible Problem	Solution
The large, multi node BLSR requires more memory for the GUI environment variables.	<p>Reset the system or user CTC_HEAP environment variable to increase the memory limits.</p> <p>See the <a href="#">“Reset the CTC_HEAP Environment Variable for Windows”</a> section on page 2-17 or the <a href="#">“Reset the CTC_HEAP Environment Variable for Solaris”</a> section on page 2-17 to enable the CTC_HEAP variable change.</p> <p><b>Note</b> This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.</p>



### 2.3.1.1 Reset the CTC\_HEAP Environment Variable for Windows

- 
- Step 1** Exit any and all open and running CTC and Netscape applications.
  - Step 2** From the Windows Desktop, right-click on My Computer and choose **Properties** in the pop-up menu.
  - Step 3** In the System Properties window, click the **Advanced** tab.
  - Step 4** Click the **Environment Variables** button to open the Environment Variables window.
  - Step 5** Click the **New** button under the User variables field or the System variables field.
  - Step 6** Type `CTC_HEAP` in the Variable Name field.
  - Step 7** Type `256` in the Variable Value field, and then click **OK** to create the variable.
  - Step 8** Click **OK** in the Environment Variables window to accept the changes.
  - Step 9** Click **OK** in the System Properties window to accept the changes.
- You may now restart the browser and CTC software.
- 

### 2.3.1.2 Reset the CTC\_HEAP Environment Variable for Solaris

- 
- Step 1** From the user shell window, kill any CTC applications.
  - Step 2** Kill any Netscape applications.
  - Step 3** In the user shell window, set the environment variable to increase the heap size: `% setenv CTC_HEAP 256`
- You may now restart the browser and CTC software in the same user shell window.
- 

## 2.3.2 Operation: Browser Stalls When Downloading CTC JAR Files From TCC+

**Symptom:** The browser stalls or hangs when downloading a CTC JAR file from the TCC+ card.

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

**Table 2-2** Browser Stalls When Downloading jar File From TCC+

Possible Problem	Solution
McAfee VirusScan software may be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.	Disable the VirusScan Download Scan feature. See the <a href="#">“Disable the VirusScan Download Scan”</a> section on page 2-18.

### 2.3.2.1 Disable the VirusScan Download Scan

- 
- Step 1** From the Windows start menu, choose **Programs > Network Associates > VirusScan Console**.
  - Step 2** Double-click the **VShield** icon listed in the VirusScan Console dialog box.
  - Step 3** Click the **Configure** button on the lower part of the Task Properties window.
  - Step 4** Click the **Download Scan** icon on the left of the System Scan Properties dialog box.
  - Step 5** Uncheck the **Enable Internet download scanning** checkbox.
  - Step 6** Click **Yes** when the warning message appears.
  - Step 7** Click **OK** on the System Scan Properties dialog box.
  - Step 8** Click **OK** on the Task Properties window.
  - Step 9** Close the McAfee VirusScan window.
- 

### 2.3.3 Operation: CTC Does Not Launch

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

[Table 2-3](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-3** *CTC Does Not Launch*

Possible Problem	Solution
The Netscape browser cache may point to an invalid directory.	Redirect the Netscape cache to a valid directory. See the <a href="#">“Redirect the Netscape Cache to a Valid Directory”</a> section on page 2-18.

#### 2.3.3.1 Redirect the Netscape Cache to a Valid Directory

- 
- Step 1** Launch Netscape.
  - Step 2** Display the **Edit** menu.
  - Step 3** Choose **Preferences**.
  - Step 4** Under the Category column on the left-hand side, go to **Advanced** and choose the **Cache** tab.
  - Step 5** Change your disk cache folder to point to the cache file location.  
The cache file location is usually C:\ProgramFiles\Netscape\Users\<yourname>\cache. The <yourname> segment of the file location is often the same as the user name.
-

## 2.3.4 Operation: Sluggish CTC Operation or Login Problems

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

Table 2-4 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-4 Sluggish CTC Operation or Login Problems**

Possible Problem	Solution
The CTC cache file may be corrupted or may need to be replaced.	Delete the CTC cache file. This operation forces the ONS 15454 to download a new set of jar files to your computer hard drive. See the “ <a href="#">Delete the CTC Cache File Automatically</a> ” section on page 2-19 or the “ <a href="#">Delete the CTC Cache File Manually</a> ” section on page 2-20.

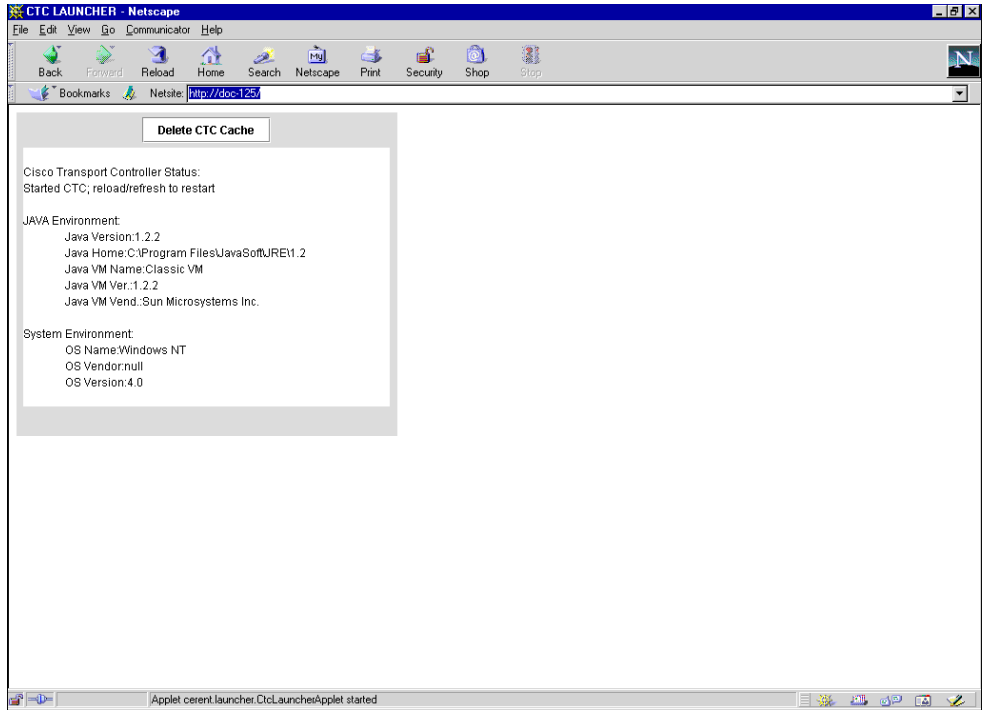
### 2.3.4.1 Delete the CTC Cache File Automatically

- Step 1** Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.
- Step 2** Close all open CTC sessions and browser windows. The PC operating system will not allow you to delete files that are in use.
- Step 3** Click the **Delete CTC Cache** button on the initial browser window to clear the CTC cache. [Figure 2-12](#) shows the Delete CTC Cache screen.



**Note** For CTC releases prior to 3.0, automatic deletion is unavailable. For CTC Cache file manual deletion, see the [Delete the CTC Cache File Manually](#)

Figure 2-12 Deleting the CTC cache



### 2.3.4.2 Delete the CTC Cache File Manually

- 
- Step 1** To delete the jar files manually, from the Windows Start menu choose **Search > For Files or Folders**.
  - Step 2** Enter \*.jar in the Search for files or folders named field on the Search Results dialog box and click **Search Now**.
  - Step 3** Click the **Modified** column on the Search Results dialog box to find the jar files that match the date when you downloaded the files from the TCC+. These files may include CTC\*.jar, CMS\*.jar, and jar\_cache\*.tmp.
  - Step 4** Highlight the files and press the keyboard **Delete** key.
  - Step 5** Click **Yes** at the Confirm dialog box.
-

## 2.3.5 Operation: Node Icon is Grey on CTC Network View

**Symptom:** The CTC network view shows one or more node icons as grey in color and without a node name.

Table 2-5 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-5 Node Icon is Grey on CTC Network View**

Possible Problem	Solution
Different CTC releases not recognizing each other.	Usually accompanied by an INCOMPATIBLE-SW alarm. Correct the core version build as described in the “ <a href="#">Operation: Different CTC Releases Do Not Recognize Each Other</a> ” section on page 2-23.
A username/password mismatch.	Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the “ <a href="#">Operation: Username or Password Do Not Match</a> ” section on page 2-24.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the “ <a href="#">Ethernet Connections</a> ” section on page 2-27.
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the “ <a href="#">EOC</a> ” section on page 1-38.

## 2.3.6 Operation: CTC Cannot Launch Due to Applet Security Restrictions

**Symptom:** The error message “Unable to launch CTC due to applet security restrictions” appears after you enter the IP address in the browser window.

Table 2-6 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-6 CTC Cannot Launch Due to Applet Security Restrictions**

Possible Problem	Solution
Did not execute the javapolicyinstall.bat file, or the java.policy file may be incomplete.	<ol style="list-style-type: none"> <li>1. Verify that you have executed the javapolicyinstall.bat file on the ONS 15454 software CD. This file is installed when you run the CTC Setup Wizard (refer to the CTC installation information in the <i>Cisco ONS 15454 Procedure Guide</i> for instructions).</li> <li>2. If you ran the javapolicyinstall.bat file but still receive the error message, you must manually edit the java.policy file on your computer. See the “<a href="#">Manually Edit the java.policy File</a>” section on page 2-21.</li> </ol>

### 2.3.6.1 Manually Edit the java.policy File

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

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

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

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

};

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

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

CTC should now start correctly.

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

## 2.3.7 Operation: Java Runtime Environment Incompatible

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

[Table 2-7](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-7 Java Runtime Environment Incompatible**

Possible Problem	Solution
Do not have the compatible JRE installed.	<p>The Java 2 Runtime Environment (JRE) contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language.</p> <p>The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. See the <a href="#">“Launch CTC to Correct the Core Version Build”</a> section on page 2-23.</p> <p>If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. <a href="#">Table 2-8</a> shows JRE compatibility with ONS 15454 software releases.</p>

**Table 2-8 JRE Compatibility**

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15454 Release 2.2.1 and earlier	Yes	No
ONS 15454 Release 2.2.2	Yes	Yes
ONS 15454 Release 3.0	Yes	Yes
ONS 15454 Release 3.1	Yes	Yes
ONS 15454 Release 3.2	Yes	Yes
ONS 15454 Release 3.3	Yes	Yes

### 2.3.7.1 Launch CTC to Correct the Core Version Build

- 
- Step 1** Exit the current CTC session and completely close the browser.
  - Step 2** Start the browser.
  - Step 3** Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.
  - Step 4** Log into CTC. The browser will download the jar file from CTC.



**Note** After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15454 and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

---

## 2.3.8 Operation: Different CTC Releases Do Not Recognize Each Other

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

[Table 2-9](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-9** *Different CTC Releases Do Not Recognize Each Other*

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the TCC+ card are incompatible.	<p>This occurs when the TCC+ software is upgraded but the PC has not yet upgraded the compatible CTC jar file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version.</p> <p><b>Note</b> Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node will not recognize the new node.</p> <p>See the <a href="#">“Launch CTC to Correct the Core Version Build”</a> section on page 2-23.</p>

### 2.3.8.1 Launch CTC to Correct the Core Version Build

- 
- Step 1** Exit the current CTC session and completely close the browser.
  - Step 2** Start the browser.
  - Step 3** Type the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.
  - Step 4** Log into CTC. The browser will download the jar file from CTC.

**Note**

After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15454 and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

## 2.3.9 Operation: Username or Password Do Not Match

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

[Table 2-10](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-10 Username or Password Do Not Match**

Possible Problem	Solution
The username or password entered do not match the information stored in the TCC+.	<p>All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes.</p> <p>For initial logon to the ONS 15454, type the <i>CISCO15</i> user name in capital letters and click <b>Login</b> (no password is required). If you are using a CTC software release prior to 3.0 and <i>CISCO15</i> does not work, type <i>cerent454</i> for the user name.</p> <p>See the “Verify Correct Username and Password” section on page 2-24.</p>

### 2.3.9.1 Verify Correct Username and Password

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



## 2.3.10 Operation: No IP Connectivity Exists Between Nodes

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

Table 2-11 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-11 No IP Connectivity Exists Between Nodes**

Possible Problem	Solution
A lost Ethernet connection.	Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the “Ethernet Connections” section on page 2-27.

## 2.3.11 Operation: DCC Connection Lost

**Symptom:** The node is usually accompanied by alarms and the nodes in the network view have a grey icon. This symptom is usually accompanied by an EOC alarm.

Table 2-12 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-12 DCC Connection Lost**

Possible Problem	Solution
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the “EOC” section on page 1-38.

## 2.3.12 Operation: Browser Login Does Not Launch Java

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

Table 2-13 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-13 Browser Login Does Not Launch Java**

Possible Problem	Solution
The PC operating system and browser are not properly configured.	Reconfigure the PC operating system and the browser. See the “Reconfigure the PC Operating System and the Browser” section on page 2-25.

### 2.3.12.1 Reconfigure the PC Operating System and the Browser

- 
- Step 1** From the Windows start menu, click **Settings > Control Panel**.
- Step 2** If **Java Plug-in Control Panel** does not appear, the JRE may not be installed on your PC.
- Run the Cisco ONS 15454 software CD.
  - Open the [CD drive]:\Windows\JRE folder.
  - Double-click the j2re-1\_3\_1\_02-win icon to run the JRE installation wizard.

- d. Follow the JRE installation wizard steps.
- Step 3** From the Windows start menu, click **Settings > Control Panel**.
- Step 4** Double-click the **Java Plug-in 1.3.1\_02** icon.
- Step 5** Click **Advanced** on the Java Plug-in Control Panel.
- Step 6** From the Java Run Time Environment menu, select **JRE 1.3 in C:\ProgramFiles\JavaSoft\JRE\1.3.1\_02**.
- Step 7** Click **Apply**.
- Step 8** On Netscape Navigator, click **Edit > Preferences**.
- Step 9** Click **Advanced > Proxies > Direct connection to the Internet > OK**.
- Step 10** Again on Netscape Navigator, click **Edit > Preferences**.
- Step 11** Click **Advanced > Cache**.
- Step 12** Confirm that the Disk Cache Folder field shows C:\ProgramFiles\Netscape\Communicator\cache for Windows 95/98/ME  
or C:\ProgramFiles\Netscape\<username>\Communicator\cache for Windows NT/2000.
- Step 13** If the Disk Cache Folder field is not correct, click **Choose Folder**.
- Step 14** Navigate to the file listed in [Step 12](#) and click **OK**.
- Step 15** Click **OK** on the Preferences window and exit the browser.
- Step 16** Temporarily disable any virus-scanning software on the computer. See the [“Operation: Browser Stalls When Downloading CTC JAR Files From TCC+”](#) section on page 2-17.
- Step 17** Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.
- Step 18** Restart the browser and log into the ONS 15454.

### 2.3.13 Connectivity: Verify PC Connection to ONS 15454 (ping)

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

[Table 2-14](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-14** *Verify PC connection to ONS 15454 (ping)*

Possible Problem	Solution
A lost connection between the PC and the ONS 1554.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC+ card. A ping command will work if the PC connects directly to the TCC+ card or uses a LAN to access the TCC+ card.  <b>Note</b> Software Release 3.0 requires the TCC+ card and does not support the TCC card. Releases 2.2, 2.2.1, and 2.2.2 support the TCC and the TCC+ cards.  See the <a href="#">“Ping the ONS 15454”</a> section on page 2-27.

### 2.3.13.1 Ping the ONS 15454

- 
- Step 1** Display the command prompt:
- If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type command prompt in the Open field of the Run dialog box, and click **OK**.
  - If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.
- Step 2** For both the Sun and Microsoft operating systems, at the prompt type:
- ```
ping [ONS 15454 IP address]
For example, ping 192.1.1.0.2.
```
- Step 3** If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a “Request timed out” message displays.
- Step 4** If the ping is successful, an active TCP/IP connection exists. Restart CTC.
- Step 5** If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation’s IP address is on the same subnet as the ONS node.
- Step 6** If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation’s NIC is illuminated.
- 

## 2.3.14 Calculate and Design IP Subnets

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

[Table 2-15](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-15 Calculate and Design IP Subnets**

| Possible Problem                                                                                  | Solution                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets. | Cisco provides a free online tool to calculate and design IP subnets. Go to <a href="http://www.cisco.com/techtools/ip_addr.html">http://www.cisco.com/techtools/ip_addr.html</a> . For information about ONS 15454 IP capability, refer to the <i>Cisco ONS 15454 Reference Manual</i> . |

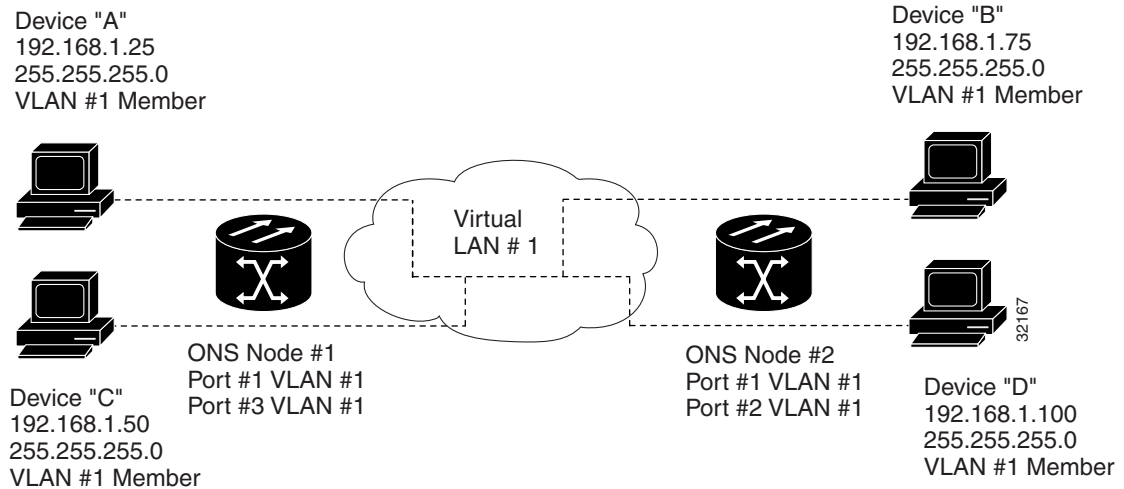
## 2.3.15 Ethernet Connections

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

[Table 2-15](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-16 Calculate and Design IP Subnets**

| Possible Problem               | Solution                                                                                                                                                                                                                            |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Improperly seated connections. | You can fix most connectivity problems in an Ethernet network by following a few guidelines. See <a href="#">Figure 2-13</a> when consulting the steps in the “ <a href="#">Verify Ethernet Connections</a> ” section on page 2-28. |
| Incorrect connections.         |                                                                                                                                                                                                                                     |

**Figure 2-13 Ethernet connectivity reference**

### 2.3.15.1 Verify Ethernet Connections

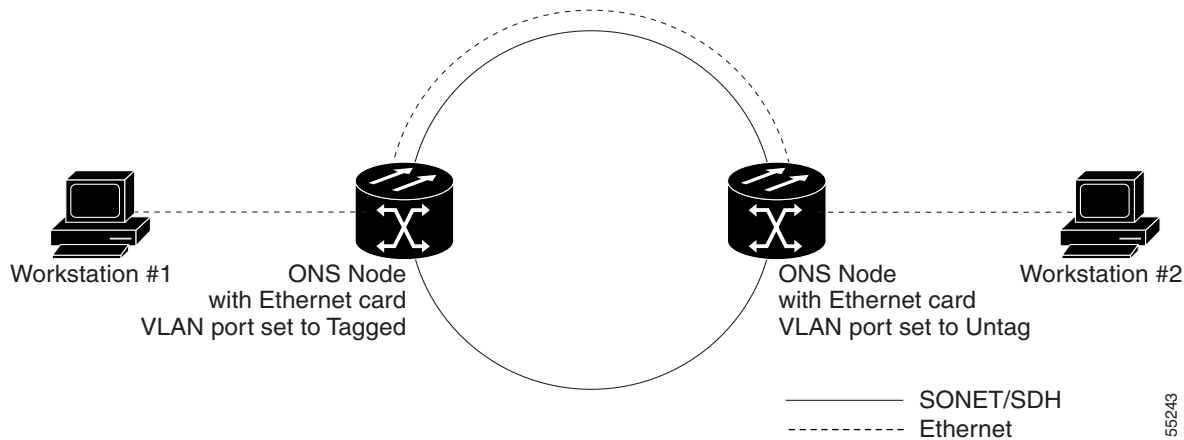
- 
- Step 1** Check for SONET alarms on the STS-N that carries the VLAN #1 Ethernet circuit. Clear any alarms by looking them up in [Chapter 1, “Alarm Troubleshooting.”](#)
- Step 2** Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in [Chapter 1, “Alarm Troubleshooting.”](#)
- Step 3** Verify that the ACT LED on the Ethernet card is green.
- Step 4** Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.
- Step 5** If no green link-integrity LED is illuminated for any of these ports:
- Verify physical connectivity between the ONS 15454s and the attached device.
  - Verify that the ports are enabled on the Ethernet cards.
  - 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.
  - 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.
  - It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Run the procedure in the [“Lamp Test for Card LEDs”](#) section on page 2-46.
- Step 6** Verify connectivity between device A and device C by pinging between these locally attached devices (see the [“Connectivity: Verify PC Connection to ONS 15454 \(ping\)”](#) section on page 2-26). If the ping is unsuccessful:
- Verify that device A and device C are on the same IP subnet.
  - Display the Ethernet card in CTC card view and click the **Provisioning > VLAN** tabs to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.
  - If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.

- Step 7** Repeat [Step 6](#) for devices B and D.
- Step 8** Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

## 2.3.16 VLAN Cannot Connect to Network Device from Untag Port

**Symptom:** Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag may have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port ([Figure 2-14](#)). They may also see a higher than normal runt packets count at the network device attached to the Untag port.

**Figure 2-14** A VLAN with Ethernet ports at Tagged and Untag



[Table 2-14](#) describes the potential cause(s) of the symptom and the solution(s).

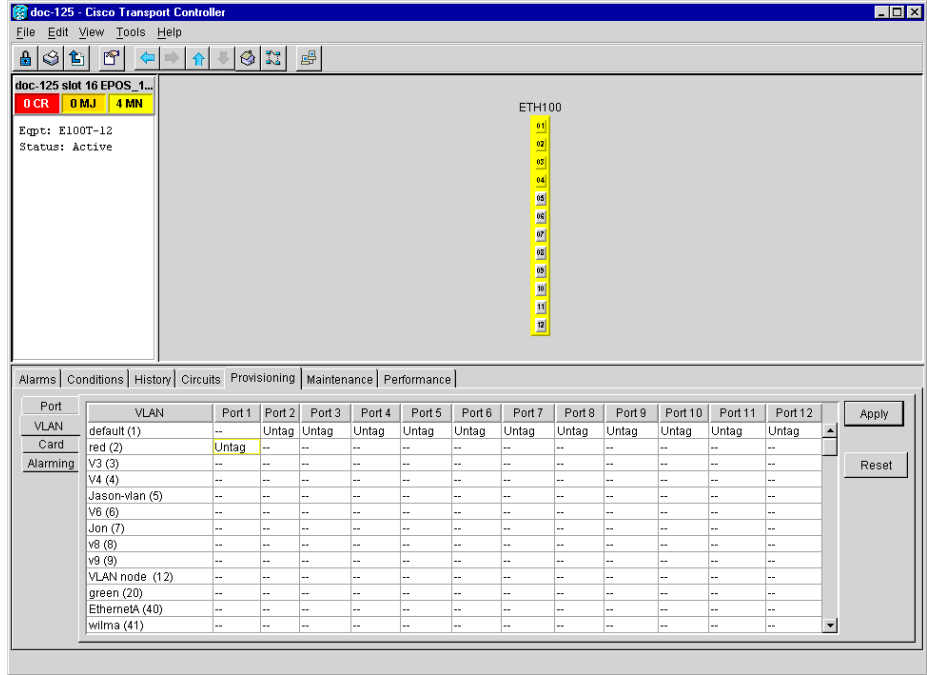
**Table 2-17 Verify PC connection to ONS 15454 (ping)**

| Possible Problem                                                                                                                                                                                     | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Tagged ONS 15454 adds the 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet. | The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevents the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with 802.1Q-compliant NIC cards will accept the tagged packets. Network devices with non-802.1Q compliant NIC cards will still drop these tagged packets. The solution may require upgrading network devices with non-802.1Q compliant NIC cards to 802.1Q-compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose 802.1Q compliance. |
| Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### 2.3.16.1 Change VLAN Port Tag and Untagged Settings

- 
- Step 1** Display the CTC card view for the Ethernet card involved in the problem VLAN.
- Step 2** Click the **Provisioning > VLAN** tabs ([Figure 2-15](#)).

Figure 2-15 Configuring VLAN membership for individual Ethernet ports



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



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

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

### 2.3.17 Cross-Connect Card Oscillator Fails

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

- SWMTXMOD against one or both cross-connect cards
- SD-L against near-end or far-end line cards
- AIS-L against far-end line cards
- RFI-L against near-end line cards

Table 2-18 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-18 Cross-Connect Card Oscillator Fails**

| Possible Problem                                    | Solution                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The XC, XCVT, or XC10G card has oscillator failure. | <ol style="list-style-type: none"> <li>1. If the Slot 8 cross-connect card is active, see the <a href="#">“Resolve the XC Oscillator Failure When Slot 8 XC Card is Active”</a> section on page 2-32.</li> <li>2. If the Slot 10 cross-connect card is active, see the <a href="#">“Resolve the XC Oscillator Failure When Slot 10 XC Card is Active”</a> section on page 2-32.</li> </ol> |

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

### 2.3.17.2 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, reseal the Slot 8 cross-connect card.
- Step 4** If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.



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

## 2.4 Circuits and Timing

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

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

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

[Table 2-19](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-19 Calculate and Design IP Subnets**

| Possible Problem                                                                                                       | Solution                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service. | An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth.<br><br>Perform the <a href="#">“Clear AIS-V on DS3XM-6 Unused VT Circuits”</a> section on <a href="#">page 2-33</a> . |

#### 2.4.1.1 Clear AIS-V on DS3XM-6 Unused VT Circuits

- Step 1** Determine the affected port.
- Step 2** Record the node ID, slot number, port number, or VT number.

- Step 3** Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.
  - Step 4** Uncheck the bidirectional box in the circuit creation window.
  - Step 5** Give the unidirectional VT circuit an easily recognizable name, such as `delete me`.
  - Step 6** Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** tabs.
  - Step 7** Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).
  - Step 8** From the Loopback Type list, choose **Facility (line)** and click **Apply**.
  - Step 9** Click **Circuits**.
  - Step 10** Find the one-way circuit you created in [Step 3](#). Select the circuit and click **Delete**.
  - Step 11** Click **Yes** in the Delete Confirmation box.
  - Step 12** Display the DS3XM-6 card in CTC card view. Click **Maintenance > DS1**.
  - Step 13** Locate the VT in Facility (line) Loopback.
  - Step 14** From the Loopback Type list, choose **None** and then click **Apply**.
  - Step 15** Click the **Alarm** tab and verify that the AIS-V alarms have cleared.
  - Step 16** Repeat this procedure for all the AIS-V alarms on the DS3XM-6 cards.
- 

## 2.4.2 Circuit Creation Error with VT1.5 Circuit

**Symptom:** You might receive an “Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at <node name>” message when trying to create a VT1.5 circuit in CTC.

[Table 2-20](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-20 Circuit Creation Error with VT1.5 Circuit**

| Possible Problem                                                                                                  | Solution                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You may have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message. | The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations will exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a UPSR or 1+1 protection group. Refer to the <i>Cisco ONS 15454 Reference Guide</i> for more information. |

## 2.4.3 Unable to Create Circuit From DS-3 Card to DS3XM-6 Card

**Symptom:** You cannot create a circuit from a DS-3 card to a DS3XM-6 card.

[Table 2-21](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-21 Unable to Create Circuit from DS-3 Card to DS3XM-6 Card**

| Possible Problem                                         | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A DS-3 card and a DS3XM-6 card have different functions. | <p>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.</p> <p><b>Note</b> You can find instructions for creating circuits in the <i>Cisco ONS 15454 Procedure Guide</i>.</p> |

## 2.4.4 DS3 Card Does Not Report AIS-P From External Equipment

**Symptom:** A DS3-12/DS3N-12/DS3-12E/DS3N-12E card does not report STS AIS-P from the external equipment/line side.

[Table 2-22](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-22 DS3 Card Does Not Report AIS-P From External Equipment**

| Possible Problem                     | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The card is functioning as designed. | <p>This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side.</p> <p>DS3-12/DS3N-12E cards have DS3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information on the PM capabilities of the DS3-12E/DS3N-12E cards, refer to the <i>Cisco ONS 15454 Procedure Guide</i>.</p> |

## 2.4.5 OC-3 and DCC Limitations

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

[Table 2-23](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-23 OC-3 and DCC Limitations**

| Possible Problem                                 | Solution                                                                                                                         |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| OC-3 and DCC have limitations for the ONS 15454. | For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the <i>Cisco ONS 15454 Procedure Guide</i> . |

## 2.4.6 ONS 15454 Switches Timing Reference

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

[Table 2-24](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-24 ONS 15454 Switches Timing Reference**

| Possible Problem                                                                                                        | Solution                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source. | The ONS 15454 internal clock operates at a Stratum 3 level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of $\pm 4.6$ ppm and a holdover stability of less than 255 slips in the first 24 hours or $3.7 \times 10^{-7}$ /day, including temperature. |
| The optical or BITS input is not functioning.                                                                           | ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.                                 |
| Sync Status Messaging (SSM) message is set to Don't Use for Sync (DUS).                                                 |                                                                                                                                                                                                                                                                                      |
| SSM indicates a Stratum 3 or lower clock quality.                                                                       |                                                                                                                                                                                                                                                                                      |
| The input frequency is off by more than 15 ppm.                                                                         |                                                                                                                                                                                                                                                                                      |
| The input clock wanders and has more than three slips in 30 seconds.                                                    |                                                                                                                                                                                                                                                                                      |
| A bad timing reference existed for at least two minutes.                                                                |                                                                                                                                                                                                                                                                                      |

## 2.4.7 Holdover Synchronization Alarm

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

[Table 2-25](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-25 Holdover Synchronization Alarm**

| Possible Problem                     | Solution                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The last reference input has failed. | The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the <a href="#">“HLDOVERSYNC” section on page 1-55</a> for a detailed description of this alarm.<br><br><b>Note</b> The ONS 15454 supports holdover timing per Telcordia standard GR-4436 when provisioned for external (BITS) timing. |

## 2.4.8 Free-Running Synchronization Mode

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

Table 2-26 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-26 Free-Running Synchronization Mode**

| Possible Problem                          | Solution                                                                                                                                                                                                                         |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No reliable reference input is available. | The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the “FRNGSYNC” section on page 1-54 for a detailed description of this alarm. |

## 2.4.9 Daisy-Chainded BITS Not Functioning

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

Table 2-27 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-27 Daisy-Chainded BITS Not Functioning**

| Possible Problem                                       | Solution                                                                                                                                                                                                                           |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Daisy-chaining BITS is not supported on the ONS 15454. | Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454. |

## 2.5 Fiber and Cabling

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

### 2.5.1 Bit Errors Appear for a Traffic Card

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

Table 2-28 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-28 Bit Errors Appear for a Line Card**

| Possible Problem                           | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Faulty cabling or low optical-line levels. | Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot cabling problems using the “ <a href="#">Network Troubleshooting Tests</a> ” section on page 2-1. Troubleshoot low optical levels using the “ <a href="#">Faulty Fiber-Optic Connections</a> ” section on page 2-38. |

## 2.5.2 Faulty Fiber-Optic Connections

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

[Table 2-29](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-29 Faulty Fiber-Optic Connections**

| Possible Problem                     | Solution                                                                                                                                                                               |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Faulty fiber-optic connections.      | Faulty fiber-optic connections can be the source of SONET alarms and signal errors. See the “ <a href="#">Verify Fiber-Optic Connections</a> ” section on page 2-38.                   |
| Faulty gigabit interface connectors. | Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the “ <a href="#">Replace Faulty Gigabit Interface Converters</a> ” section on page 2-40. |
| Faulty CAT-5 cables.                 | Faulty CAT-5 cables can be the source of SONET alarms and signal errors. See the “ <a href="#">Crimp Replacement CAT-5 Cables</a> ” section on page 2-42.                              |



### Warning

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

### 2.5.2.1 Verify Fiber-Optic Connections

- 
- Step 1** Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.  
SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.
- Step 2** Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

- Step 3** Check that the single-mode fiber power level is within the specified range:
- Remove the receive (Rx) end of the suspect fiber.
  - Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.
  - Determine the power level of fiber with the fiber-optic power meter.
  - Verify the power meter is set to the appropriate wavelength for the optical card being tested (either 1310 nm or 1550 nm depending on the specific card).
  - Verify that the power level falls within the range specified for the card; see the [“Optical Card Transmit and Receive Levels”](#) section on page 2-43.
- Step 4** If the power level falls below the specified range:
- Clean or replace the fiber patch cords. If possible, do this for the OC-N card you are working on and the far-end card.
  - Clean the optical connectors on the card. If possible, do this for the OC-N card you are working on and the far-end card.
  - Ensure that the far-end transmitting card is not an ONS intermediate range (IR) card when an ONS long range (LR) card is appropriate.  
IR cards transmit a lower output power than LR cards.
  - Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

**Caution**


---

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

---

- If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):
  - Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
  - Excessive number of fiber connectors; connectors take approximately 0.5 dB each.
  - Excessive number of fiber splices; splices take approximately 0.5 dB each.

**Note**


---

These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

---

- Step 5** If no power level shows on the fiber, the fiber is bad or the transmitter on the optical card failed.
- Check that the Transmit (Tx) and Receive (Rx) fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.
  - Clean or replace the fiber patch cords. If possible, do this for the OC-N card you are working on and the far-end card.
  - Retest the fiber power level.
  - If the replacement fiber still shows no power, replace the optical card.

**Step 6** If the power level on the fiber is above the range specified for the card, ensure that an ONS long-range (LR) card is not being used when an ONS intermediate-range (IR) card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter will be too powerful for the receiver on the receiving OC-N card.

Receiver overloads occur when maximum receiver power is exceeded.



**Tip**

To prevent overloading the receiver, use an attenuator on the fiber between the ONS OC-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS OC-N cards. Refer to the attenuator documentation for specific instructions.



**Tip**

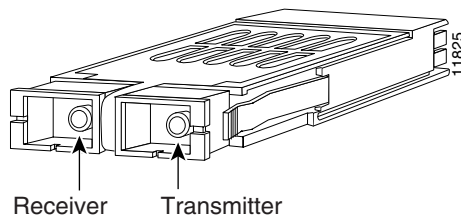
Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

## 2.5.2 Replace Faulty Gigabit Interface Converters

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

GBICs can be installed or removed while the card and shelf assembly are powered and running. GBIC transmit failure is characterized by a steadily blinking Fail LED on the Gigabit Ethernet (E1000-2/E1000-2-G) card. [Figure 2-16](#) shows a GBIC.

**Figure 2-16** A gigabit interface converter (GBIC)



**Warning**

**Class 1 laser product**



**Warning**

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

**Step 1** Disconnect the network interface fiber-optic cable from the GBIC SC connector and replace the protective plug.



**Step 2** Release the GBIC from the card-interface by simultaneously squeezing the two plastic tabs, one on each side of the GBIC.

**Step 3** Slide the GBIC out of the Gigabit Ethernet front-panel slot.



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

**Step 4** Remove the new GBIC from its protective packaging.

**Step 5** Check the part number to verify that the GBIC is the correct type for your network.



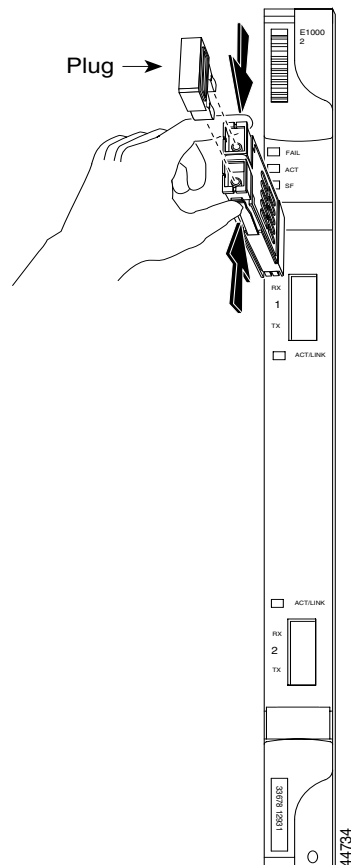
**Caution** Check the label on the GBIC carefully. The two GBIC models look similar.

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



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

**Figure 2-17** Installing a GBIC on the E1000-2/E1000-2-G card



**Step 7** Slide the GBIC through the front flap until you hear a click.

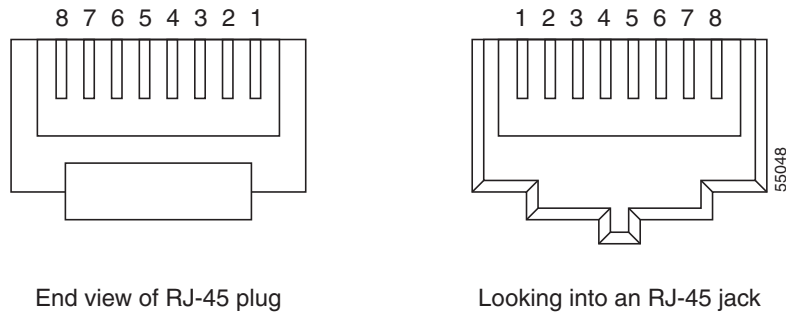
The click indicates that the GBIC is locked into the slot.

- Step 8** When you are ready to attach the network interface fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

### 2.5.2.3 Crimp Replacement CAT-5 Cables

You can crimp your own CAT-5 cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a straight-through cable when connecting an ONS 15454 to a router or workstation. Use CAT 5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. [Figure 2-18](#) shows the layout of an RJ-45 connector. [Figure 2-19](#) shows the layout of a straight-through cable and [Figure 2-20](#) shows the layout of a cross-over cable.

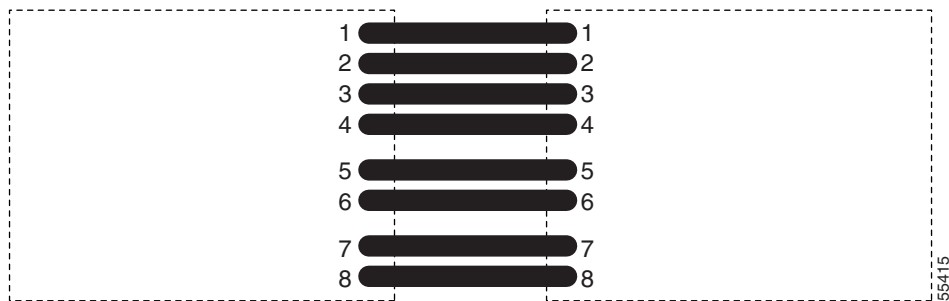
**Figure 2-18 RJ-45 pin numbers**



End view of RJ-45 plug

Looking into an RJ-45 jack

**Figure 2-19 A straight-through cable layout**



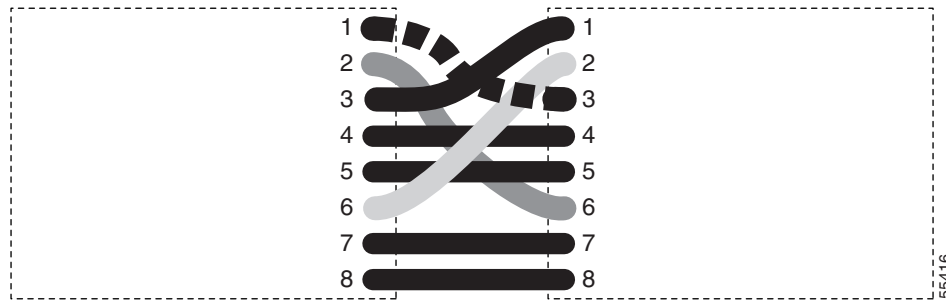
**Table 2-30 Straight-through cable pinout**

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

**Table 2-30** Straight-through cable pinout (continued)

| Pin | Color       | Pair | Name | Pin |
|-----|-------------|------|------|-----|
| 7   | white/brown | 4    |      | 7   |
| 8   | brown       | 4    |      | 8   |

**Figure 2-20** A cross-over cable layout



**Table 2-31** Cross-over cable pinout

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



**Note**

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

## 2.5.3 Optical Card Transmit and Receive Levels

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

**Table 2-32** Optical Card Transmit and Receive Levels

| Optical card         | Rx            | Tx            |
|----------------------|---------------|---------------|
| OC3 IR 4/STM1SH 1310 | -8 to -28 dBm | -8 to -15 dBm |
| OC12 IR/STM4 SH 1310 | -8 to -28 dBm | -8 to -15 dBm |
| OC12 LR/STM4 LH 1310 | -8 to -28 dBm | +2 to -3 dBm  |
| OC12 LR/STM4 LH 1550 | -8 to -28 dBm | +2 to -3 dBm  |

**Table 2-32 Optical Card Transmit and Receive Levels (continued)**

| Optical card    | Rx            | Tx            |
|-----------------|---------------|---------------|
| OC12/STM4-4     | -8 to -28 dBm | +2 to -3 dBm  |
| OC48 IR 1310    | 0 to -18 dBm  | 0 to -5 dBm   |
| OC48 LR 1550    | -8 to -28 dBm | +3 to -2 dBm  |
| OC48 AS LR 1550 | -8 to -28 dBm | +3 to -2 dBm  |
| OC48 ELR DWDM   | -8 to -28 dBm | 0 to -2 dBm   |
| OC192 LR 1550   | -9 to -17 dBm | +10 to +7 dBm |

## 2.6 Power and LED Tests

This section provides the “Power Supply Problems” section on page 2-44, the “Power Consumption for Node and Cards” section on page 2-45, and the “Lamp Test for Card LEDs” section on page 2-46.

### 2.6.1 Power Supply Problems

**Symptom:** Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

Table 2-33 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-33 Power Supply Problems**

| Possible Problem                   | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loss of power or low voltage.      | The ONS 15454 requires a constant source of DC power to properly function. Input power is -48 VDC. Power requirements range from -42 VDC to -57 VDC.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Improperly connected power supply. | <p>A newly installed ONS 15454 that is not properly connected to its power supply will not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site.</p> <p>A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the <b>Provisioning &gt; General</b> tabs and change the <i>Date</i> and <i>Time</i> fields.</p> <p>See the “Isolate the Cause of Power Supply Problems” section on page 2-45.</p> |

**Caution**

Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

**Warning**

**When working with live power, always use proper tools and eye protection.**

**Warning**

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

### 2.6.1.1 Isolate the Cause of Power Supply Problems

- Step 1** If a single ONS 15454 show signs of fluctuating power or power loss:
- a. Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.
  - b. Verify that the power cable is #12 or #14 AWG and in good condition.
  - c. Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.
  - d. Verify that 20A fuses are used in the fuse panel.
  - e. Verify that the fuses are not blown.
  - f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.
  - g. Verify that the DC power source has enough capacity to carry the power load.
  - h. If the DC power source is battery-based:
    - Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.
    - Check the age of the batteries. Battery performance decreases with age.
    - Check for opens and shorts in batteries, which may affect power output.
    - If brownouts occur, the power load and fuses may be too high for the battery plant.
- Step 2** If multiple pieces of site equipment show signs of fluctuating power or power loss:
- a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer’s documentation for specific instructions.
  - b. Check for excessive power drains caused by other equipment, such as generators.
  - c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

## 2.6.2 Power Consumption for Node and Cards

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

Table 2-34 describes the potential cause(s) of the symptom and the solution(s).

**Table 2-34 Power Consumption for Node and Cards**

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

## 2.6.3 Lamp Test for Card LEDs

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

[Table 2-35](#) describes the potential cause(s) of the symptom and the solution(s).

**Table 2-35** *Lamp Test for Card LEDs*

| Possible Problem | Solution                                                                                                                                                                                                                                                                                           |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Faulty LED       | A lamp test verifies that all the card LEDs work. Run this diagnostic test as part of the initial ONS 15454 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order.<br><br>See the <a href="#">“Verify Card LED Operation”</a> section on page 2-46. |

### 2.6.3.1 Verify Card LED Operation

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

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

---



## Replace Hardware

---

This chapter provides procedures for replacing Cisco ONS 15454 hardware.

Every section is a procedure.

1. [Switch Traffic and Replace an In-Service Cross-Connect Card, page 3-2](#)—Complete this procedure to replace and in-service cross-connect card.
2. [Reset the TCC+ With a Card Pull, page 3-5](#)—Complete this procedure as needed to reset the TCC+ by performing a card pull.
3. [Replace the Air Filter, page 3-5](#)—Complete this procedure to replace a reusable or disposable air filter.
4. [Determine Replacement Hardware Compatibility, page 3-11](#)—Complete this procedure to verify replacement hardware compatibility.
5. [Replace the Fan-Tray Assembly, page 3-13](#)—Complete this procedure to replace the fan-tray assembly.
6. [Replace the Alarm Interface Panel, page 3-15](#)—Complete this procedure to replace the alarm interface panel (AIP).
7. [Replace the Electrical Interface Assembly, page 3-20](#)—Complete this procedure to replace the electrical interface assembly (EIA).

## 3.1 Switch Traffic and Replace an In-Service Cross-Connect Card

|                                |                                                           |
|--------------------------------|-----------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an in-service cross-connect card. |
| <b>Tools/Equipment</b>         | Replacement cross-connect card                            |
| <b>Prerequisite Procedures</b> | None                                                      |
| <b>Required/As Needed</b>      | As needed                                                 |
| <b>Onsite/Remote</b>           | Onsite                                                    |



### Warning

**Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**



### Caution

Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, follow the steps below to switch the XC/XCVT/XC10G card to standby prior to removing the card from the node.



### Note

An improper removal (IMPROPRMVL) alarm is raised whenever a card pull is performed, unless the card is deleted in CTC first. The alarm will clear after the card replacement is complete.



### Note

In a UPSR, pulling the active XC/XCVT/XC10G without a lockout will cause UPSR circuits to switch.

### Step 1

Log into the node where you will perform the XC/XCVT/XC10G card replacement:

- a. From your PC, start Netscape or Internet Explorer.
- b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.



### Note

If you are logging into ONS 15454 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node with an older release, you receive an INCOMPATIBLE-SW alarm and the IP address of the login node will display instead of the node name. To check the software version of a node, select **About CTC** from the CTC Help menu.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments.

- c. In the Login dialog box, type your name and password (both are case sensitive).
- d. Each time you log into an ONS 15454, you can make selections on the following login options:
  - *Node Name*—Displays the IP address entered in the web browser and a pull-down menu of previously-entered ONS 15454 IP addresses. You can select any ONS 15454 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.



- *Additional Nodes*—Displays a list of login node groups that were created. To create a login node group or add additional groups, see the *Cisco ONS 15454 Procedure Guide*.)



**Note** Topology hosts that were created in previous ONS 15454 releases by modifying the `ctc.ini` file are displayed as a “Topology Host” group under Additional Nodes.

- *Exclude Dynamically Discovered Nodes*—Check this box to view only the ONS 15454 (and login node group members, if any) entered in the *Node Name* field. Nodes linked to the *Node Name* ONS 15454 through the DCC are not displayed. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.

e. Click **Login**.

**Step 2** Ensure the working span is active on both local and remote nodes:

- In node view, click the **Maintenance > Ring** tabs.
- Locate the applicable span.
- In the West Line and East Line columns, the working/active span is identified by (Work/Act).

**Step 3** Ensure the working span is carrying error-free traffic (no SD or SF alarms present). Display the network view and click the **Alarms** tab to display alarms.

**Step 4** Lockout the protection span according to the specific protection scheme:

- Lockout the protection span in a BLSR protection scheme:
  - In node (default) view, click the **Maintenance > Ring** tabs.
  - Locate the applicable span.
  - In the West Line and East Line columns, the working/active span is identified by (Work/Act). Place a lockout on the East and West cards of the nodes adjacent to the XC switch node; for example, to switch the XC on Node B, place a lockout on the West card of Node A and on the East card of Node C, no lockout is necessary on Node B. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.  
 <-----East [Node A] West-----East [Node B] West-----East [Node C] West----->
- Lockout the protection span in a 1+1 protection scheme:
  - In node (default) view, click the **Maintenance > Protection** tabs.
  - Choose the affected 1+1 protection group from the Protection Groups window.
  - In the Selected Group window, the working and protect spans appear. Choose the **protect/standby card** and choose **Lockout** from the inhibit switching row.
  - Click **Yes** on the confirmation dialog box.



**Note** An XC/XCVT/XC10G reset can cause a linear 1+1 OC-N protection switch or a BLSR protection switch.

c. Lockout the protection span in a UPSR protection scheme:

- In network view, right-click the span where you want to switch UPSR traffic. Choose **Circuits** from the shortcut menu.
- On the Circuits on Span dialog box, choose **FORCE**.

**Caution**


---

The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

---

- Step 5** When the protection span has been locked out, determine the active XC/XCVT/XC10G card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

**Note**


---

You can also place the cursor over the card graphic to display a pop-up identifying the card as active or standby.

---

- Step 6** Switch the active XC/XCVT/XC10G card to standby:
- a. In the node view, click the **Maintenance > XC Cards** tabs.
  - b. Under Cross Connect Cards, choose **Switch**.
  - c. Click **Yes** on the Confirm Switch dialog box.

**Note**


---

After the active XC/XCVT/XC10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

---

- Step 7** Physically remove the new standby XC/XCVT/XC10G card from the ONS 15454.

- Step 8** Insert the replacement XC/XCVT/XC10G card into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

- Step 9** Release the protection lockout(s) applied in [Step 4](#):

- a. Log into the node where you will clear the Lock Out.
- b. Click the **Maintenance > Protection** tabs.
- c. Under Protection Groups, click the protection group that contains the card you want to clear.
- d. Under Selected Group, click the card you want to clear.
- e. From Inhibit Switching, click **Unlock**.
- f. Click **Yes** on the confirmation dialog box.

The lock out is cleared.

---

## 3.2 Reset the TCC+ With a Card Pull

|                                |                                           |
|--------------------------------|-------------------------------------------|
| <b>Purpose</b>                 | Use this procedure to reseal a TCC+ card. |
| <b>Tools/Equipment</b>         | None                                      |
| <b>Prerequisite Procedures</b> | None                                      |
| <b>Required/As Needed</b>      | As needed                                 |
| <b>Onsite/Remote</b>           | Onsite                                    |



**Note** To determine whether you have an active or standby TCC+, position the cursor over the TCC+ card graphic to display the status.

- Step 1** Ensure that the TCC+ you want to reset is in standby mode. On the TCC+ card, the ACT/STBY (Active/Standby) LED is amber when the TCC+ is in standby mode.
- Step 2** When the TCC+ is in standby mode, unlatch both the top and bottom ejector levers on the TCC+ card.
- Step 3** Physically pull the card at least partly out of the slot until the lighted LEDs turn off.
- Step 4** Wait 30 seconds. Reinsert the card and close the ejector levers.



**Note** The TCC+ will take several minutes to reboot and will display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about LED behavior during TCC+ reboots.

## 3.3 Replace the Air Filter

|                                |                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | The following procedure describes how to replace reusable and disposable air filters. |
| <b>Tools/Equipment</b>         | Spare air filters                                                                     |
| <b>Prerequisite Procedures</b> | None                                                                                  |
| <b>Required/As Needed</b>      | As needed                                                                             |
| <b>Onsite/Remote</b>           | Onsite                                                                                |



**Warning** Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.



**Note** Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

- Step 1** To replace the reusable air filter, complete the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) task on page 3-6.

- Step 2** To replace the disposable air filter, complete the “[Inspect and Replace the Disposable Air Filter](#)” task on [page 3-8](#).
- 

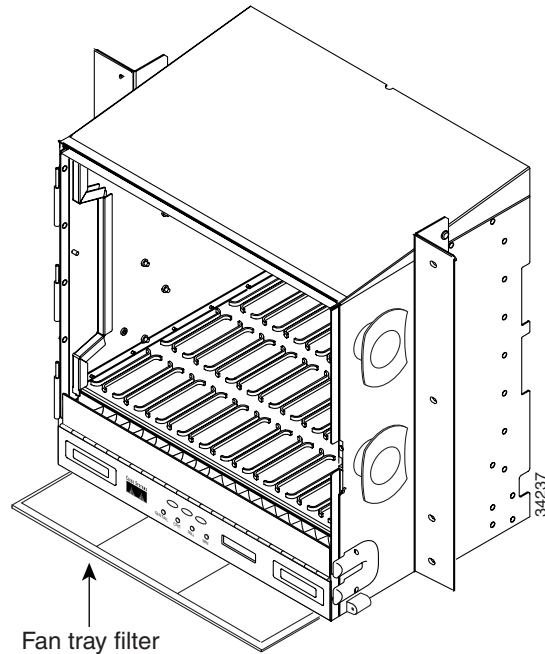
### 3.3.1 Inspect, Clean, and Replace the Reusable Air Filter

|                                |                                                                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This task ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf. |
| <b>Tools/Equipment</b>         | Vacuum or detergent and water faucet, spare filter, pinned hex key                                                                                  |
| <b>Prerequisite Procedures</b> | None                                                                                                                                                |
| <b>Required/As Needed</b>      | Inspection required every 30 days. Clean as needed.                                                                                                 |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                              |

---

- Step 1** Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.
- Step 2** If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that may have collected on the filter and proceed to [Step 5](#). [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:
- Step 3** Open the front door of the shelf assembly.
- Open the front door lock.  
The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
  - Press the door button to release the latch.
  - Swing the door open.
- Step 4** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 5](#):
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - Secure the dangling end of the ground strap to the door or chassis with tape.

**Figure 3-1** A reusable fan-tray air filter in an external filter bracket (front door removed)



- Step 5** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 6** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 7** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 8** Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that may have collected on the filter.
- Step 9** Visually inspect the air filter material for dirt and dust.
- Step 10** If the reusable air filter contains 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 (spare filters should be kept in stock) and also replace the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.



**Note** Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

- Step 11** If you washed the filter, allow it to completely air dry for at least eight hours.



**Warning** Do not put a damp filter back in the ONS 15454.

- a. If the air filter is installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.
- b. If the filter is installed beneath the fan-tray assembly, remove the fan-tray assembly, and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.



**Caution** If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.



**Note** On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

- Step 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** If you replace the door, also reattach the ground strap.
- Step 15** Close and lock the door.

## 3.3.2 Inspect and Replace the Disposable Air Filter

|                                |                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This task ensures that the air filter is free from dirt and dust to allow optimum air flow and prevent dirt and dust from entering the ONS 15454. |
| <b>Tools/Equipment</b>         | Extra filters, pinned hex key                                                                                                                     |
| <b>Prerequisite Procedures</b> | None                                                                                                                                              |
| <b>Required/As Needed</b>      | Inspection required every 30 days. Replace as needed.                                                                                             |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                            |



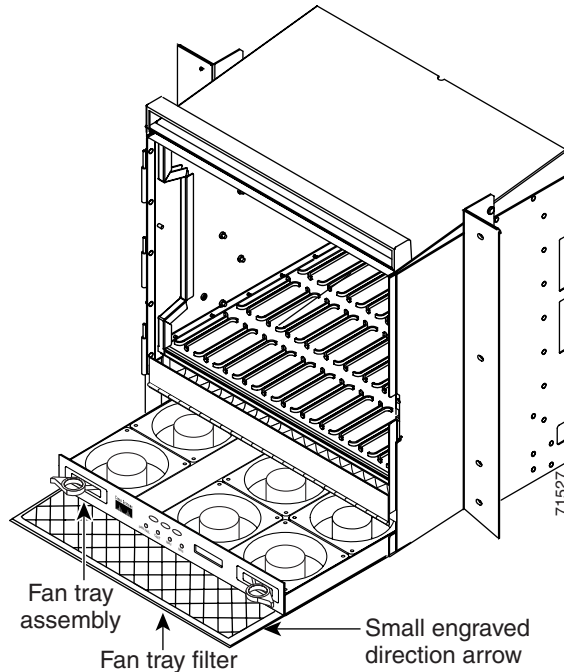
**Note** The disposable air filter is installed beneath the fan-tray assembly only, so you must remove the fan-tray assembly to inspect and replace the disposable air filter.

- Step 1** Verify that you are replacing a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. NEBS 3E and earlier versions of the ONS 15454 use a disposable air filter.
- Step 2** Open the front door of the shelf assembly.
- Open the front door lock.
 

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
  - Press the door button to release the latch.
  - Swing the door open.
- Step 3** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 4](#):
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 4** Push the outer side of the handles on the fan-tray assembly to expose the handles.

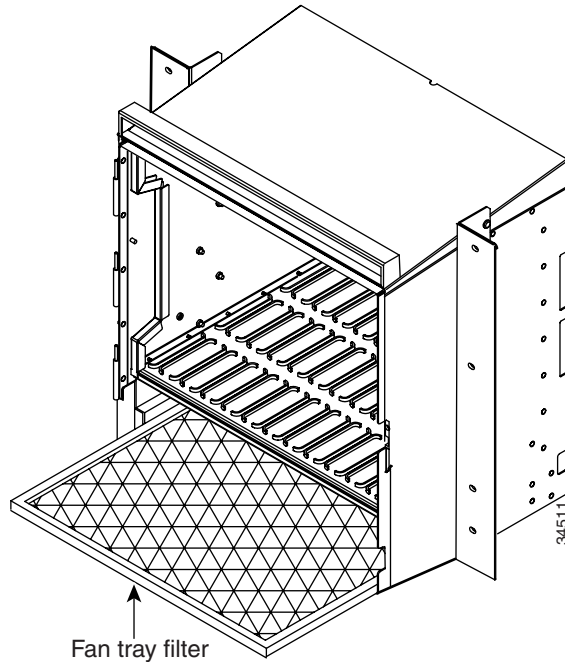
- Step 5** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 3-2).

**Figure 3-2** Inserting or removing the fan-tray assembly (front door removed)



- Step 7** Gently remove the air filter from the shelf assembly (Figure 3-3). Be careful not to dislodge any dust that may have collected on the filter.
- Step 8** Visually inspect the white filter material for dirt and dust.
- Step 9** If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter by sliding the filter into the bottom of the shelf assembly. Make sure that the front of the filter is flush with the front of the shelf assembly and that the air flow indicators on the filter point upwards.

**Figure 3-3** Inserting or removing a disposable fan-tray air filter (front door removed)



- Step 10** Slide the fan-tray assembly into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 11** To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.
- Step 12** Rotate the retractable handles back into their compartments.
- Step 13** If you replace the door, also reattach the group strap.
- Step 14** Close and lock the door.
-



## 3.4 Determine Replacement Hardware Compatibility

|                                |                                                                          |
|--------------------------------|--------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure determines replacement hardware compatibility.            |
| <b>Tools/Equipment</b>         | None                                                                     |
| <b>Prerequisite Procedures</b> | None                                                                     |
| <b>Required/As Needed</b>      | Required when replacing the fan-tray assembly and alarm interface panel. |
| <b>Onsite/Remote</b>           | Both                                                                     |



### Caution

The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.



### Note

The 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC10G, OC-192, and OC-48AS cards.



### Note

The 5A alarm interface panel (AIP) (73-7665-XX) is required when installing the 15454-FTA3 fan-tray assembly.

### Step 1

Review [Table 3-1](#) to ensure you have compatible components when replacing the fan-tray assembly or the AIP and note the alarms that will occur when an incompatible combination of hardware is installed.



### Note

If you need to determine the hardware that has been installed on a node, click the inventory tab in node view.

Table 3-1 Incompatibility Alarms

| Shelf Assembly <sup>1</sup> | Fan Tray <sup>2</sup> | AIP <sup>3</sup> | 10G Cards <sup>4</sup> | Ethernet Cards <sup>5</sup> | Alarms                         |
|-----------------------------|-----------------------|------------------|------------------------|-----------------------------|--------------------------------|
| —                           | —                     | No fuse          | —                      | —                           | MEA on AIP                     |
| NEBS3E or NEBS3             | 2A                    | 2A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 2A                    | 2A               | Yes                    | —                           | MEA on 10G                     |
| NEBS3E or NEBS3             | 2A                    | 5A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 2A                    | 5A               | Yes                    | —                           | MEA on 10G                     |
| NEBS3E or NEBS3             | 5A                    | 2A               | No                     | —                           | MEA on fan tray                |
| NEBS3E or NEBS3             | 5A                    | 2A               | Yes                    | —                           | MEA on fan tray and 10G cards  |
| NEBS3E or NEBS3             | 5A                    | 5A               | No                     | —                           | None                           |
| NEBS3E or NEBS3             | 5A                    | 5A               | Yes                    | —                           | MEA on 10G                     |
| ANSI                        | 2A                    | 2A               | No                     | —                           | None                           |
| ANSI                        | 2A                    | 2A               | Yes                    | 2.5G compatible             | MEA on fan tray, AIP, Ethernet |
| ANSI                        | 2A                    | 2A               | Yes                    | 10G compatible              | MEA on fan tray, AIP           |
| ANSI                        | 2A                    | 5A               | No                     | Either                      | None                           |
| ANSI                        | 2A                    | 5A               | Yes                    | 2.5G compatible             | MEA on fan tray, Ethernet      |
| ANSI                        | 2A                    | 5A               | Yes                    | 10G compatible              | MEA on fan tray                |
| ANSI                        | 5A                    | 2A               | No                     | Either                      | MEA on AIP                     |
| ANSI                        | 5A                    | 2A               | Yes                    | 2.5G compatible             | MEA on AIP, Ethernet           |
| ANSI                        | 5A                    | 2A               | Yes                    | 10G compatible              | MEA on AIP                     |
| ANSI                        | 5A                    | 5A               | No                     | Either                      | None                           |
| ANSI                        | 5A                    | 5A               | Yes                    | Either                      | None                           |

- 15454-SA-ANSI (P/N: 800-19857-01) = ONS 15454 Release 3.1 and later shelf assembly, 15454-SA-NEBS3E (P/N: 800-07149-xx) or 15454-SA-NEBS3 (P/N: 800-06741-xx) = shelf assemblies released before ONS 15454 Release 3.1
- 5A Fan Tray = 15454-FTA3 (P/N: 800-19858-xx) or 15454-FTA3-T (P/N: 800-21448-xx), 2A Fan Tray = 15454-FTA2 (P/Ns: 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx)
- 5A AIP (P/N: 73-7665-01), 2A AIP (P/N: 73-5262-01)
- 10G cards = XC-10G, OC-192, OC-48AS
- 2.5G compatible Ethernet cards = E1000-T, E1000-2, E1000T-G, E10002-G, G1000-4  
10G compatible Ethernet cards = E1000T-G, E10002-G, G1000-4

**Step 2** See the “[Replace the Fan-Tray Assembly](#)” section on page 3-13 to replace the fan-tray assembly or the “[Inspect and Replace the Disposable Air Filter](#)” section on page 3-8 to replace the alarm interface panel.

## 3.5 Replace the Fan-Tray Assembly

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities. You can remove the fan-tray assembly using the retractable handles and replace it by pushing until it plugs into the receptacle on the back panel.

|                                |                                                                         |
|--------------------------------|-------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing FTA with a new FTA.                 |
| <b>Tools/Equipment</b>         | None                                                                    |
| <b>Prerequisite Procedures</b> | <a href="#">Determine Replacement Hardware Compatibility, page 3-11</a> |
| <b>Required/As Needed</b>      | As needed                                                               |
| <b>Onsite/Remote</b>           | Onsite                                                                  |



### Caution

The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.



### Caution

Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.



### Note

The 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

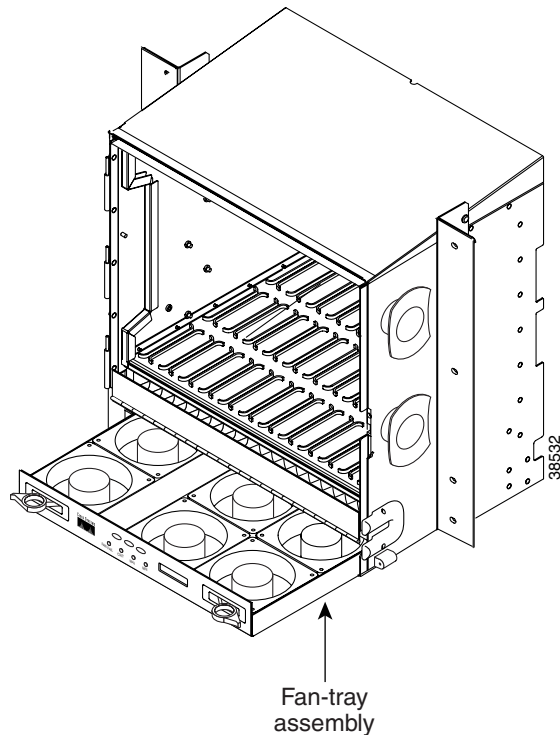
- 
- Step 1** Open the front door of the shelf assembly:
- Open the front door lock.
 

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
  - Press the door button to release the latch.
  - Swing the door open.
- Step 2** Remove the front door (optional). If you do not want to remove the door, proceed to [Step 3](#):
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
  - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
  - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Fold out the retractable handles at the outside edges of the fan tray.
- Step 5** Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. [Figure 3-4](#) shows the location of the fan tray.

## Replace the Fan-Tray Assembly

- Step 7** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
- If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [“Replace the Air Filter” section on page 3-5](#).
- Step 8** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 9** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.
- Step 10** If you replace the door, also reattach the ground strap.
- Step 11** Close and lock the door.

**Figure 3-4** Removing or replacing the fan-tray assembly (front door removed)



## 3.6 Replace the Alarm Interface Panel

|                                |                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing AIP with a new AIP on an in-service system without affecting traffic |
| <b>Tools/Equipment</b>         | #2 phillips screw driver                                                                                 |
| <b>Prerequisite Procedures</b> | <a href="#">Determine Replacement Hardware Compatibility, page 3-11</a>                                  |
| <b>Required/As Needed</b>      | As needed                                                                                                |
| <b>Onsite/Remote</b>           | Onsite                                                                                                   |


**Caution**

Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.


**Caution**

There is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Assistance Center (TAC) at 877-323-7368 when prompted to do so in the procedure.


**Caution**

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


**Note**

Perform this procedure in a maintenance window. Resetting the active TCC+ can cause a service disruption of less than 50 ms to OC-N or DS-N traffic. Resetting the active TCC+ will cause a service disruption of 3–5 minutes on all Ethernet traffic due to Spanning Tree Reconvergence.

**Step 1**

Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

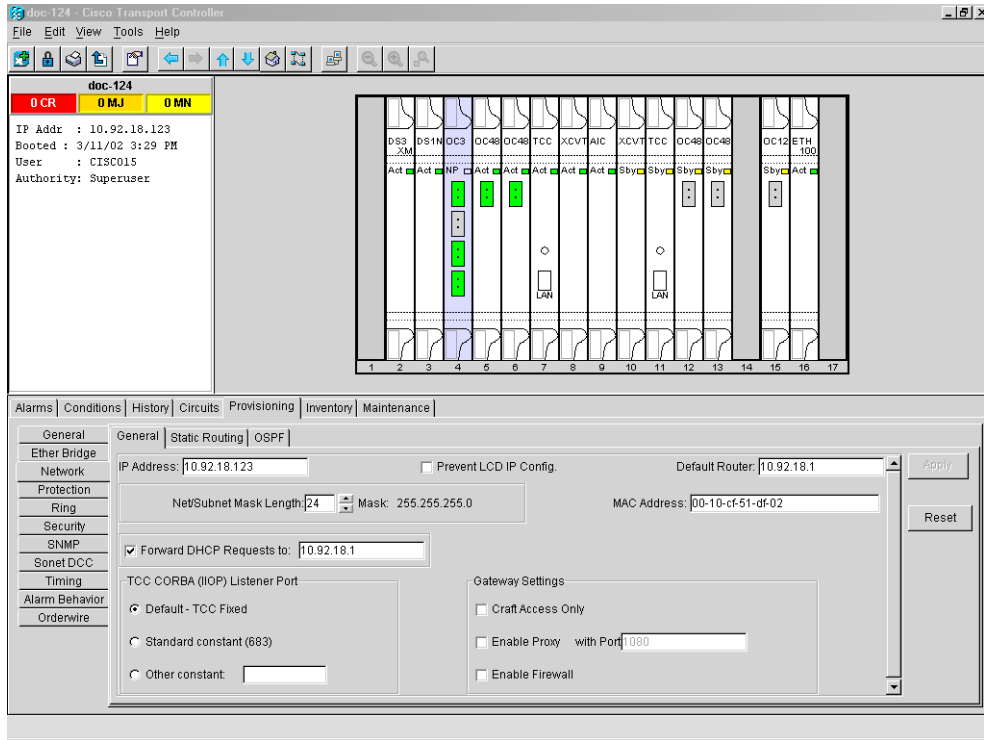
- a. Log into CTC. See [Step 1](#) in the “[Switch Traffic and Replace an In-Service Cross-Connect Card](#)” procedure on page 3-2 for instructions.
- b. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
- c. If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to [Step 2](#).

**Step 2**

Record the MAC address of the old AIP:

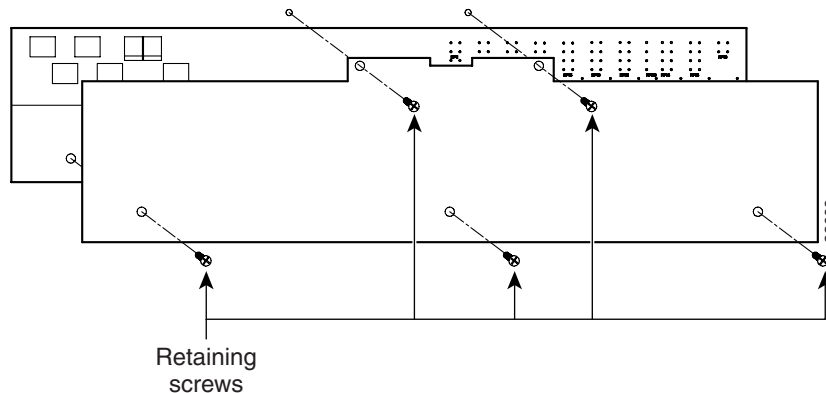
- a. Log into the node where you will replace the AIP. For login procedures, see the Cisco ONS 15454 Procedure Guide.
- b. In node view, click on the **Provisioning > Network** tabs.
- c. Record the MAC address shown in the General tab in [Figure 3-5](#).

Figure 3-5 Find the MAC address



- Step 3** Call Cisco TAC at 877-323-7368 for assistance in replacing the AIP and maintaining the original MAC address.
- Step 4** Unscrew the five screws that hold the lower backplane cover in place (Figure 3-6).
- Step 5** Grip the lower backplane cover and gently pull away from the backplane.

Figure 3-6 Lower backplane cover



- Step 6** Unscrew the two screws that hold the AIP cover in place.
- Step 7** Grip the cover and gently pull away from the backplane.



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

**Step 8** Grip the AIP and gently pull away from the backplane.

**Step 9** Disconnect the fan-tray assembly power cable from the AIP.

**Step 10** Set the old AIP aside for return to Cisco.



**Caution** The type of shelf the AIP resides in will determine the version of AIP that will replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) currently uses the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and lower currently use the 2A AIP (P/N: 73-5262-01).



**Caution** Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857); doing so will cause a blown fuse on the AIP.

**Step 11** Attach the fan-tray assembly power cable to the new AIP.

**Step 12** Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

**Step 13** Replace the AIP cover over the AIP and secure the cover with the two screws.

**Step 14** Replace the lower backplane cover and secure the cover with the five screws.

**Step 15** In node view, click on the **Provisioning > Network** tabs.



**Caution** Cisco recommends TCC+ resets be performed in a maintenance window to avoid any potential service disruptions.

**Step 16** Reset the standby TCC+:

- a. In node view, right click on the standby TCC+ card and choose **Reset Card**.
- b. Click **Yes** on the Resetting Card dialog box. As the card resets, a loading (Ldg) indication will appear on the card in CTC.



**Note** The reset will take approximately five minutes. Do not perform any other steps until the reset is complete.

**Step 17** Reset the active TCC+:

- a. In node view, right click on the active TCC+ card and choose **Reset Card**.
- b. Click **Yes** on the Resetting Card dialog box. As the card resets, a Ldg indication will appear on the card in CTC.



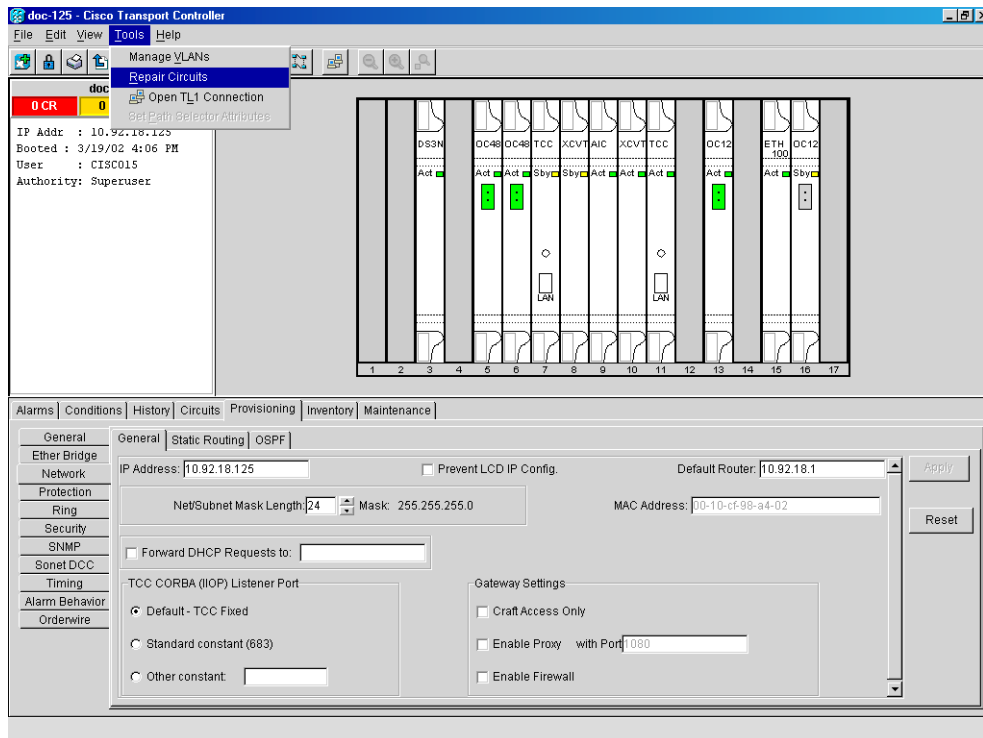
**Note** The reset will take approximately five minutes and CTC will lose its session with the node.

**Step 18** Click **File** from the menu bar and choose **Exit** to exit the CTC session.

## Replace the Alarm Interface Panel

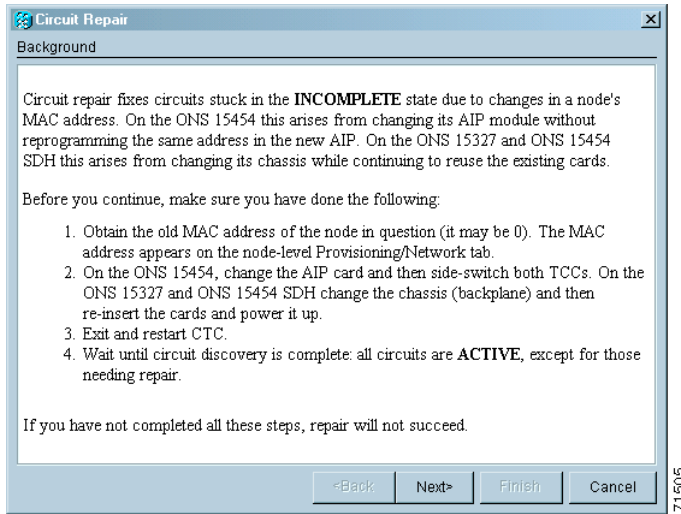
- Step 19** Login back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes pull-down menu.
- Step 20** Record the new MAC address:
- In node view, click on the **Provisioning > Network** tabs.
  - Record the MAC address shown in the General tab.
- Step 21** In node view, click on the **Circuits** tab. Note that all circuits listed are in an INCOMPLETE state.
- Step 22** In node view, choose **Tools** from the menu bar and click **Repair Circuits** (Figure 3-7). The Circuit Repair dialog box is displayed.

**Figure 3-7 Repair Circuits in the Menu Bar**



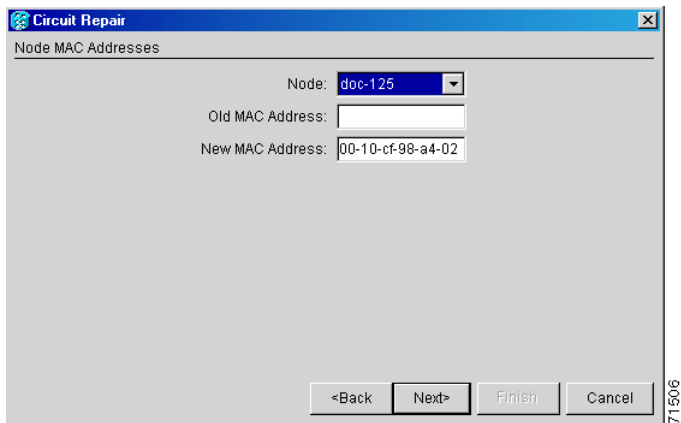
- Step 23** Read the instructions in the Circuit Repair dialog box (Figure 3-8). If all the steps in the dialog box have been completed, click **Next>**. Ensure you have the old and new MAC addresses.



**Figure 3-8** Repairing circuits

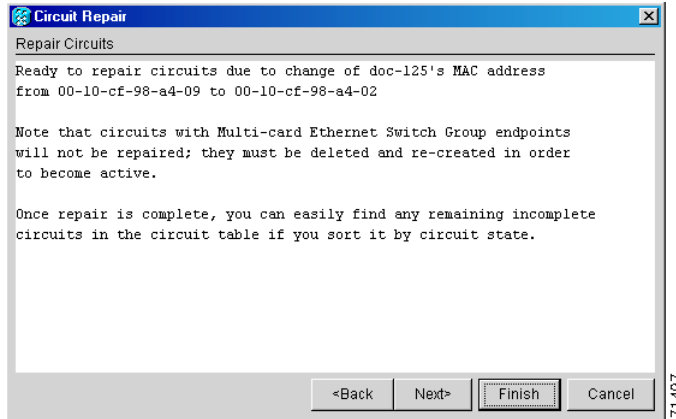
**Step 24** The Node MAC Addresses dialog box displays (Figure 3-9):

- a. From the Node pull down menu, choose the name of the node where you replaced the AIP.
- b. In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.
- c. Click **Next**.

**Figure 3-9** Recording the old MAC address before replacing the AIP

**Step 25** The Repair Circuits dialog box displays (Figure 3-10). Read the information in the dialog box and click **Finish**.

Figure 3-10 Circuit repair information



**Note** The CTC session will freeze until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

- Step 26** When the circuit repair is complete, the Circuits Repaired dialog box will display.
- Step 27** Click **OK**.
- Step 28** In the new node view, click on the **Circuits** tab. Note that all circuits listed are in an ACTIVE state. If all circuits listed are not in an ACTIVE state, call Cisco TAC at 877-323-7368 for assistance.
- Step 29** Return the defective AIP. You must follow the standard Return Material Authorizations (RMA) procedures; call (800) 553-NETS (6387) if you do not have an RMA number.

## 3.7 Replace the Electrical Interface Assembly

|                                |                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>                 | This procedure replaces an existing EIA with a new EIA.                                                                                                               |
| <b>Tools/Equipment</b>         | <ul style="list-style-type: none"> <li>• #2 phillips screw driver</li> <li>• BNC insertion and removal tool (Optional; for use with high-density BNC EIAs)</li> </ul> |
| <b>Prerequisite Procedures</b> | None                                                                                                                                                                  |
| <b>Required/As Needed</b>      | As needed                                                                                                                                                             |
| <b>Onsite/Remote</b>           | Onsite                                                                                                                                                                |

- Step 1** To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 3-6).
- Step 2** Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.



---

**Note** If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

---

- Step 3** If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.
- Step 4** If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull the EIA panel away from the backplane.



---

**Note** Attach backplane sheet metal covers whenever EIAs are not installed.

---

- Step 5** Line up the connectors on the new EIA with the mating connectors on the backplane.
- Step 6** Gently push the EIA until both sets of connectors fit together snugly.
- Step 7** Replace the nine perimeter screws that you removed while removing the backplane cover.
- Step 8** If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.
- Step 9** Reattach the lower backplane cover.
-

■ Replace the Electrical Interface Assembly



---

## A

AIC card

ENVALRM [1-8](#)

external facility alarm [1-44](#)

AIP

alarms list [1-3](#)

different cover types [1-74](#)

MEA alarm [1-74](#)

MFGMEM alarm [1-77](#)

air filter, replace [3-5](#)

AIS [1-11](#)

AIS-L [1-11](#)

AIS-P [1-12, 2-35](#)

AIS-V [1-12, 2-33](#)

alarm indication signal see AIS

alarms

alarms are indexed individually by name

TL1 [1-1](#)

alarm troubleshooting [1-1 to 1-107](#)

AMI coding [1-59, 1-60](#)

APSB [1-13](#)

APSCDFLTK [1-13](#)

APSC-IMP [1-14](#)

APSCINCON [1-15](#)

APSCM [1-15](#)

APSCNMIS [1-16](#)

APSM [1-17](#)

APS see protection switching

ARP [2-29](#)

asynchronous mapping [1-82](#)

AUTOLSROFF [1-18](#)

automatic protection switching see protection switching

automatic reset [1-18](#)

AUTORESET [1-18](#)

AUTOSW-AIS [1-19](#)

AUTOSW-LOP (STSMON) [1-19](#)

AUTOSW-LOP (VT-MON) [1-19](#)

AUTOSW-PDI [1-20](#)

AUTOSW-SDBER [1-20](#)

AUTOSW-SFBER [1-20](#)

AUTOSW-UNEQ (STSMON) [1-20](#)

AUTOSW-UNEQ (VT-MON) [1-20](#)

---

## B

B8ZS [1-59](#)

B8ZS coding [1-60](#)

battery

high-voltage alarm [1-37, 1-38](#)

low voltage alarm [1-38](#)

BER [1-87, 1-89, 1-91, 1-92](#)

bit error rate see BER

BITS

daisy-chained [2-37](#)

errors [2-36](#)

holdover timing [2-36](#)

loss of frame [1-59](#)

BKUPMEMP [1-20](#)

BLSR

exercise ring failure [1-43](#)

far-end protection line failure [1-53](#)

improper configuration (alarms) [1-13](#)

ring switch failure [1-47](#)

squelch alarm [1-95](#)

BLSROSYNC

similarity to APSCDFLTK [1-13](#)  
 troubleshooting procedure [1-22](#)  
 BNC connector [1-85, 1-103](#)  
 browser  
   applet security restrictions [2-21](#)  
   cannot launch Java [2-25](#)  
   stalls during download [2-17](#)

---

## C

cache, redirect Netscape cache [2-18](#)  
 CARLOSS  
   cause of TPTFAIL [1-102](#)  
   E series [1-23](#)  
   E series Ethernet [1-23](#)  
   G1000-4 card [1-26](#)  
 carrier loss [1-23, 1-26](#)  
 CAT-5 cables [2-42](#)  
 CBIT framing [2-15](#)  
 circuits  
   AIS-V alarm on DS3XM-6 card [2-33](#)  
   identify failure points [2-3](#)  
   VT1.5 creation error [2-34](#)  
 CLDRESTART [1-28](#)  
 CLETOP [1-106](#)  
 CONCAT [1-29](#)  
 conditions indexed individually by name  
 CONTBUS-A [1-30](#)  
 CONTBUS-A-18 [1-31](#)  
 CONTBUS-B [1-31](#)  
 CONTBUS-B-18 [1-33](#)  
 cross-connect cards  
   main payload bus failure [1-35](#)  
   reset [1-34](#)  
   side (manual) switch [1-35](#)  
   switching matrix failure [1-97](#)  
   test [2-8](#)  
 CTC  
   applet not loaded [2-25](#)

  applet security restrictions [2-21](#)  
   grey node icon [2-21](#)  
   list of alarms [1-1](#)  
   log in [3-2](#)  
   log-in errors [2-17, 2-21, 2-24, 2-25](#)  
   loss of TCP/IP connection [1-25](#)  
   release interoperability problems [2-23](#)  
   username and password mismatch [2-24](#)  
   verifying PC connection [2-26](#)  
 CTNEQPT-PBPROT [1-33](#)  
 CTNEQPT-PBWORK [1-35](#)  
 cyclic redundancy checking [1-20](#)  
 cyclic redundancy checking (CRC) [1-20](#)

---

## D

database memory exceeded [1-36](#)  
 DATAFLT [1-36](#)  
 DCC  
   channel loss [1-38](#)  
   connection loss [2-25](#)  
   delete a DCC termination [1-57](#)  
   disable autodiscovery [3-3](#)  
   limitations with OC-3 [2-35](#)  
 default K alarm [1-13](#)  
 DISCONNECTED [2-26](#)  
 DS3-MISM [1-37](#)  
 DS3XM-6 card  
   AIS-V alarm and unused VT circuits [2-33](#)  
   FEAC features [2-14](#)  
 DS-N cards  
   AIS-P not reported [2-35](#)  
   DS-3 LOF [1-52](#)  
   DS-3 LOS [1-53](#)  
   facility loopback example [2-2](#)  
   failure to switch [1-44](#)  
   frame format mismatch [1-37](#)  
   idle DS-3 signal [1-51](#)  
   line alarms [1-107](#)

LOF [1-60](#)  
 loopback facility alarm [1-70](#)  
 loopback signal received [1-69](#)  
 loss of signal [1-66](#)  
 remote alarm indication [1-84](#)  
 terminal loopback alarm [1-71](#)  
 test [2-5](#)

## E

east/ west mismatch alarm [1-41](#)  
 EC1-12 card  
   LOF [1-61](#)  
   loopback facility alarm [1-70](#)  
   LOS [1-67](#)  
   terminal loopback alarm [1-71](#)  
 EHIBATVG-A [1-37](#)  
 EHIBATVG-B [1-38](#)  
 EIA [2-6, 2-14](#)  
 electrical cabling [2-5](#)  
 ELWBATVG-A [1-38](#)  
 ELWBATVG-B [1-38](#)  
 EOC [1-38](#)  
 EPROM [1-77](#)  
 EQPT  
   BKUMEMP [1-21](#)  
   troubleshooting procedure [1-40](#)  
 EQPT-MISS [1-41](#)  
 equipment failure [1-40, 1-41, 1-50](#)  
   DS-3 [1-51](#)  
 Ethernet  
   carrier loss [1-23, 1-26](#)  
   configuring VLANs [2-31](#)  
   connectivity problems [2-27](#)  
   replace faulty GBIC [2-40](#)  
   Tag/Untag port connectivity [2-29](#)  
   troubleshooting connections [2-27](#)  
 E-W-MISMATCH [1-41](#)  
 EXCCOL [1-43](#)

excess collisions [1-43](#)  
 EXERCISE-RING-FAIL [1-43](#)  
 exercise ring failure [1-43](#)  
 EXERCISE-SPAN-FAIL [1-44](#)  
 exercise span failure [1-44](#)  
 EXT [1-44](#)

## F

facility loopback  
   create on a DS-N card [2-4](#)  
   definition [2-2](#)  
   test a destination DS-N card [2-11](#)  
   test a source DS-N card [2-4](#)  
   test the circuit [2-5](#)  
 FAILTOSW [1-44](#)  
 FAILTOSW-PATH [1-45](#)  
 FAILTOSWR [1-47](#)  
 FAILTOSWS [1-48](#)  
 FAN [1-48](#)  
 fan-tray assembly  
   high temperature error [1-49](#)  
   MEA [1-76](#)  
   missing unit alarm [1-41](#)  
 FEAC [2-14 to 2-16](#)  
 FEAC, alarms [2-16](#)  
 FE-AIS [1-49](#)  
 FE-DS1-MULTLOS [1-50](#)  
 FE-DS1-SNGLLOS [1-50](#)  
 FE-DS3-SA [1-50](#)  
 FE-EQPT-NSA [1-51](#)  
 FE-IDLE [1-51](#)  
 FE-LOCKOUT [1-52](#)  
 FE-LOF [1-52](#)  
 FE-LOS [1-53](#)  
 FEPRLF [1-53](#)  
 fiber-optic connections [2-38](#)  
 flash manager [1-20](#)  
 flow rate [1-43](#)

FORCED-REQ [1-53](#)  
 force switch [1-34, 1-36, 1-53](#)  
 frame format [1-37](#)  
 free run synchronization [1-54](#)  
 FRNGSYNC  
   alarm troubleshooting [1-54](#)  
   and SYNCTHIRD [1-100](#)  
   general troubleshooting [2-37](#)  
 FSTSYNC [1-54](#)

---

## G

G1000-4 card  
   alarms [1-102](#)  
   CARLOSS alarm [1-26](#)  
   carrier loss [1-26](#)  
   LPBKTERMINAL alarm [1-72](#)  
 GBIC [2-40](#)

---

## H

hairpin circuit  
   create on source node [2-7](#)  
   definition [2-3](#)  
   perform on source node [2-7](#)  
   test hairpin loopback [2-8](#)  
 hard reset (card pull) [3-5](#)  
 hardware replacement compatibility [3-11](#)  
 HITEMP [1-54](#)  
 HLDOVERSYNC  
   alarm troubleshooting [1-55](#)  
   and SYNCTHIRD [1-100](#)  
   general troubleshooting [2-36](#)  
 holdover synchronization [1-55](#)

---

## I

idle signal condition [1-51](#)

improper card removal [1-56](#)  
 IMPROPRMVL [1-55](#)  
 INCOMPATIBLE-SW [1-57, 2-23](#)  
 Internet Explorer [3-2](#)  
 interoperability [2-23](#)  
 INVMACADDR [1-58](#)  
 IP  
   connectivity [2-25](#)  
   designing subnets [2-27](#)  
   select address for log in [3-2](#)

---

## J

Java  
   browser will not launch [2-25](#)  
   Jave Runtime Environment [2-22](#)  
 JRE  
   description [2-22](#)  
   incompatibility [2-22](#)  
   launch failure [2-25](#)

---

## K

KB-PASSTHR [1-58](#)  
 k bytes [1-13, 1-14, 1-58](#)

---

## L

lamp test [2-46](#)  
 LED test [2-46](#)  
 line card see traffic card  
 line coding [1-55, 1-59, 1-60](#)  
 line framing [1-59, 1-60](#)  
 lockout  
   locate [1-45](#)  
   lockout raised (condition) [1-52](#)  
   perform a lock out [1-17](#)  
   switch request equipment alarm [1-58](#)



LOCKOUT-REQ [1-58](#)

## LOF

BITS [1-59](#)

DS-1 [1-60](#)

DS3XM-6 [1-60](#)

EC-1 [1-61](#)

OC-N [1-62](#)

LOGBUFR90 [1-62](#)

LOGBUFROVFL [1-63](#)

## log-in errors

applet security restrictions [2-21](#)

browser login does not launch Java [2-25](#)

browser stalls when downloading .jar file [2-17](#)

no DCC connection [2-25](#)

no IP connectivity [2-25](#)

username/password mismatch [2-24](#)

login node groups [3-3](#)

## loopback

alarms [1-69, 1-71, 1-72, 1-73](#)

description [2-1](#)

see also facility loopback

terminal loopback description [2-2](#)

terminal loopback on destination DS-N [2-9, 2-11](#)

LOP-P [1-63](#)

LOP-V [1-65](#)

## LOS

BITS [1-66](#)

DS-3, DS3XM-6, DS-1 [1-66](#)

EC-1 [1-67](#)

OC-N [1-68](#)

loss of frame see LOP

loss of pointer see LOP

loss of signal see FE-LOS

LPBKDS1FEAC [1-69](#)

LPBKDS3FEAC [1-69](#)

## LPBKFACILITY

DS-N [1-70](#)

OC-N [1-71](#)

## LPBKTERMINAL

DS-N or G1000-4 [1-72](#)

OC-N [1-71, 1-72](#)

---

## M

### MAC address

data memory failure [1-77](#)

invalid [1-58](#)

mismatch [2-30](#)

MAN-REQ [1-73](#)

MANRESET [1-73](#)

manual switch [1-46, 1-61, 1-62, 1-64, 1-65, 2-9](#)

manual switch see protection switching

MEA [1-74](#)

MEM-GONE [1-76](#)

MEM-LOW [1-77](#)

### memory buffer

90% full [1-63](#)

exceeded [1-63](#)

MFGMEM [1-77](#)

---

## N

### Netscape Navigator

clear cache [2-18](#)

log in [3-2](#)

### network testing

see hairpin circuits

see loopback

NIC card [2-26, 2-30](#)

NOT-AUTHENTICATED [1-78](#)

NOT-AUTHENTICATED (alarm) [2-24](#)

---

## O

### OC-N cards

see also specific card names

bit errors [2-37](#)

lockout request failure [1-58](#)  
 LOF [1-62](#)  
 loopback caveat [2-1](#)  
 OC-192 temperature alarm [1-18](#)  
 OC-3 and DCC limitations [2-35](#)  
 terminal loopback condition [1-72](#)  
 transmit and receive levels [2-43](#)

---

## P

passwords

login [3-2](#)  
 password/ username mismatch [2-24](#)

path trace [1-101](#)

PDI-P [1-79](#)

PEER-NORESPONSE [1-81](#)

ping [1-95](#)

ping an ONS 15454 [2-26](#)

PLM-P [1-81](#)

PLM-V [1-82](#)

power

consumption [2-45](#)  
 NE power failure (connector A) [1-83](#)  
 NE power failure (connector B) [1-84](#)  
 supply [2-44](#)

PRC-DUPID [1-83](#)

protection group, delete [1-57](#)

protection switching

APS channel failure on protect card [1-53](#)  
 APS channel mismatch [1-15](#)  
 APS mode mismatch failure [1-17](#)  
 byte failure [1-13](#)  
 clear a forced switch [1-36](#)  
 clear a force switch [1-34](#)  
 clear a manual switch [1-46](#)  
 clear the manual switch condition [1-73](#)  
 cross-connect cards [1-35](#)  
 inconsistent APS code [1-15](#)  
 invalid k bytes in APS [1-14](#)

lockout switch condition [1-58](#)

manual switch [2-8](#)

ring switch failure [1-47](#)

see also force switch

see also manual switch

span switch failure [1-48](#)

UPSR alarms [1-19, 1-20](#)

PWR-A [1-83](#)

PWR-B [1-84](#)

---

## R

RAI [1-84](#)

RCVR-MISS [1-85](#)

RDI-P [1-85](#)

receive levels [2-43](#)

remote fault indication see RFI

reset

automatic [1-18](#)  
 hard (reset)/ card pull [3-5](#)

RFI

line level [1-85](#)  
 path level [1-86](#)  
 VT level [1-86, 1-87](#)

RING-MISMATCH [1-87](#)

rings

ID mismatch [1-87](#)  
 see BLSR  
 see UPSR

---

## S

SD-L [1-87](#)

SD-P [1-89](#)

severities, alarm [1-9](#)

SF-L [1-90](#)

SF-P [1-92](#)

SFTWDWN-FAIL [1-93](#)

side switch [2-8, 2-9](#)

side switch see manual switch

side switch see protection switching

signal degrade [1-20](#)

signal failure [1-20, 1-90, 1-92](#)

signal label mismatch failure see SMLF [1-81](#)

SLMF [1-79, 1-81](#)

SMB connector [1-85, 1-103](#)

SNTP [1-95](#)

SNTP-HOST [1-94](#)

soft reset see CTC reset

software

- determine version [3-2](#)
- incompatible alarm [3-2](#)
- PC/ TCC+ version mismatch [1-57](#)
- version mismatch among multiple nodes [3-2](#)

SONET

- improper APS alarm [1-14](#)
- line layer (maintenance span) [1-11](#)
- path layer [1-12](#)
- VT layer [1-12, 1-65](#)

SQUELCH [1-95](#)

SSM

- failure [1-96](#)
- synchronization traceability alarm [1-97](#)
- timing switch [2-36](#)

SSM-FAIL [1-96](#)

SSM-STU [1-96](#)

STS concatenation error [1-29](#)

STSMON [1-19, 1-20](#)

SWFTDWN [1-93](#)

switching see protection switching

SWMTXMOD [1-97](#)

SWTOPRI [1-99](#)

SWTOSEC [1-99](#)

SWTOTHIRD [1-99, 1-100](#)

synchronization status messaging see SSM

SYNCPRI [1-99](#)

SYNCSEC [1-100](#)

SYNCTHIRD [1-100](#)

SYSBOOT [1-101](#)

---

## T

TCC+ card

- communication failure (TCC+ card to traffic card) [1-30](#)
- communication failure (TCC+ to TCC+) [1-31](#)
- communication loss (TCC+ to TCC+) [1-33](#)
- communication loss (TCC+ to traffic card) [1-31](#)
- flash memory exceeded [1-36](#)
- flash memory problems [1-20](#)
- hard reset [3-5](#)
- jar file download problem [2-17](#)
- loss of signal from BITS [1-66](#)
- low memory [1-77](#)
- memory capacity exceeded [1-77](#)
- software download failure [1-93](#)

TCP/IP [1-25, 2-26](#)

Telcordia

- default severities [1-1](#)
- signal degrade definition [1-87, 1-89](#)
- signal failure definition [1-90, 1-92](#)
- trouble categories [1-9](#)

temperature

- fan-tray assembly alarm [1-49](#)
- high-temperature alarm [1-54](#)
- OC-192 alarm [1-18](#)

testing

- see lamp test
- see loopback
- see power

timing alarms

- change timing reference [1-57](#)
- loss of primary reference [1-99](#)
- loss of third reference [1-100](#)
- switching to secondary timing source [1-99](#)
- switching to third timing source [1-99](#)
- synchronization [1-54, 1-55](#)

timing reference failure [1-54](#)  
 timing reference switch [2-35](#)  
 TIM-P [1-101](#)  
 TL1 alarms [1-1](#)  
 topology hosts [3-3](#)  
 TPTFAIL [1-102](#)  
 traffic cards see DS-N cards, OC-N cards, EC1-12 card  
 transmission failure [1-103](#)  
 transmit levels [2-43](#)  
 TRMT [1-103](#)  
 TRMT-MISS [1-103](#)  
 troubleclearing see troubleshooting  
 troubleshooting [2-1 to 2-46](#)  
     see also alarm troubleshooting  
     see also loopback  
     conditions [1-9](#)  
     severities [1-9](#)  
     tests overview [2-1](#)  
     trouble notifications [1-9](#)

---

## U

UNEQ  
     AUTOSW-UNEQ (STSMON) [1-20](#)  
     AUTOSW-UNEQ (VT-MON) [1-20](#)  
 UNEQ-P [1-104](#)  
 UNEQ-V [1-105](#)  
 UPSR  
     AIS alarm [1-19](#)  
     exercise ring failure [1-43](#)  
     failed switch path [1-45](#)  
     LOP alarm [1-19](#)  
     PDI alarm [1-20](#)  
     SD alarm [1-20](#)  
     signal failure alarm [1-20](#)  
 username/password mismatch [2-24](#)

---

## V

VirusScan [2-17, 2-18](#)  
 voltage see battery  
 VT1.5 creation error [2-34](#)  
 VT-MON [1-20](#)

---

## W

west/ east misconnection alarm [1-41](#)

---

## X

XC10G card  
     manual switch see manual switch  
 XCVT card  
     manual switch see manual switch