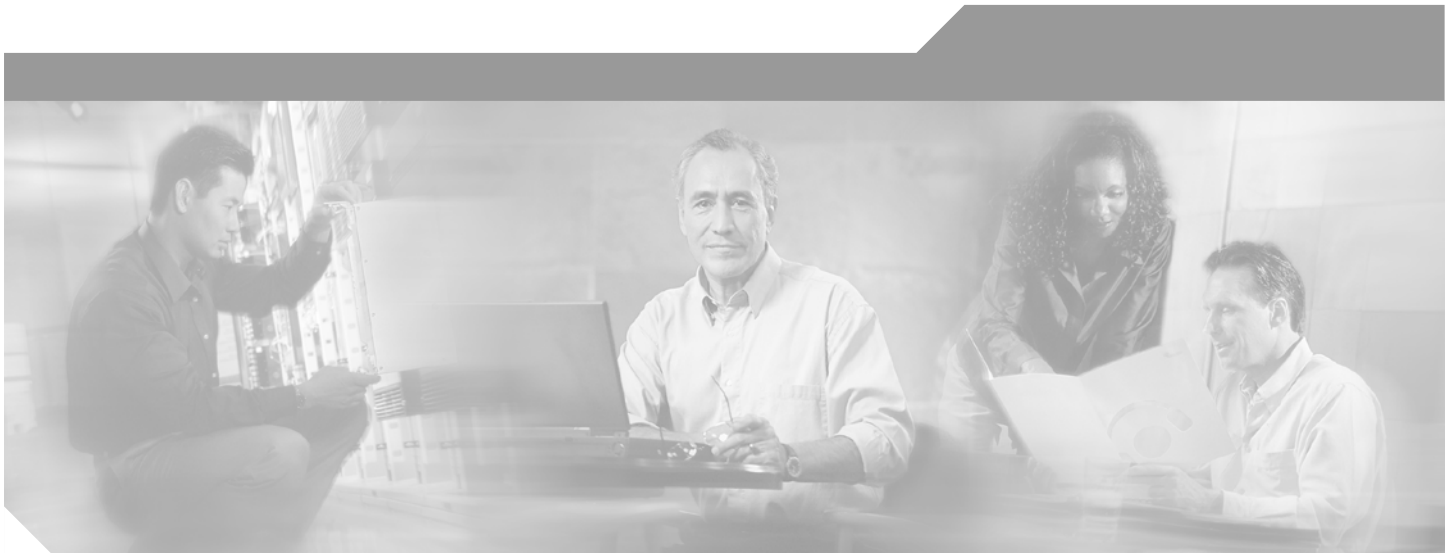


Cisco ONS 15454 SONET and DWDM Troubleshooting Guide

Product and Documentation Release 4.7
Last Updated: August 21, 2007

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

Customer Order Number: DOC-7816538=
Text Part Number: 78-16538-01

Cisco ONS 15454 SONET and DWDM Troubleshooting Guide

About This Guide

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

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

Revision History

Date	Notes
03/28/2007	Revision History Table added for the first time
08/21/2007	Updated About this Guide chapter

This section provides the following information:

Document Objectives

This guide gives general troubleshooting instructions, alarm troubleshooting instructions, error messages, performance monitoring parameters, and simple network management (SNMP) applications for the Cisco ONS 15454. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

The *Cisco ONS 15454 SONET and DWDM Troubleshooting Guid*e is organized into the following chapters:

- Chapter 1, "General Troubleshooting," provides methods to discover hardware errors, such as failed ports, that adversely affect signal traffic; it also gives typical software problems and their solutions.
- Chapter 2, "Alarm Troubleshooting," provides indexes, descriptions, and troubleshooting methods for all alarms and conditions generated by the network.
- Chapter 3, "Error Messages," provides a comprehensive list of all ONS error messages and their identification numbers.
- Chapter 4, "Performance Monitoring," provides definitions of PM parameters for all ONS 15454 cards.
- Chapter 5, "SNMP," describes the ONS 15454 implementation of simple network management protocol.

Related Documentation

Use the *Cisco ONS 15454 SONET and DWDM Troubleshooting Guide* in conjunction with the following referenced publications:

- *Cisco ONS 15454 DWDM Installation and Operations Guide*
- *Cisco ONS 15454 Release 4.7 Network Element Defaults*
- *Cisco ONS 15454 SDH Release 4.7 Network Element Defaults*
- *Release Notes for Cisco ONS 15454 Release 4.7*
- *Release Notes for Cisco ONS 15454 SDH Release 4.7*
- *Cisco ONS 15454 SONET and SDH TL1 Quick Reference Guide, Release 4.7*
- *Release Notes for the Cisco ONS 15454 Release 4.7*
- *Release Notes for the Cisco ONS 15454 SDH Release 4.7*

Refer to the following standards documentation referenced in this publication:

- Telcordia GR-253 CORE

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 systems. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

General Troubleshooting

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

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454. To troubleshoot specific ONS 15454 alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for, contact the Cisco Technical Assistance Center (1 800 553-2447).

Note Release 4.7 is DWDM only. It supports all DWDM, transponder (TXP), and muxponder (MXP) cards but not optical, electrical, fibre storage, or Ethernet cards.

This chapter includes the following sections on network problems:

- 1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks, page 1-2—Describes loopbacks, which you can use to test circuit paths through the network or logically isolate faults.
- 1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks, page 1-5—Explains how to use loopbacks tests described in"Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on MXP or TXP circuits.
- 1.3 Troubleshooting DWDM Circuit Paths With G.709 Monitoring, page 1-20—Explains how to use performance monitoring (PM) and threshold crossing alerts (TCA) to locate signal degrades on DWDM circuit paths.

Note To perform a DWDM network acceptance test, refer to NTP-G16 in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

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

- 1.4 Using CTC Diagnostics, page 1-28—Explains how to perform card LED tests, download a diagnostic file for Technical Support, and create a diagnostic standby BLSR circuit.
- 1.5 Restoring the Database and Default Settings, page 1-33—Provides procedures for restoring software data and restoring the node to the default setup.

- 1.6 PC Connectivity Troubleshooting, page 1-39—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- 1.7 CTC Operation Troubleshooting, page 1-45—Provides troubleshooting procedures for CTC login or operation problems.
- 1.8 Circuits and Timing, page 1-58—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- 1.9 Fiber and Cabling, page 1-63—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- 1.10 Power Supply Problems, page 1-72—Provides troubleshooting procedures for power supply problems.

1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks

Use loopbacks to test newly created SONET circuits before running live traffic or to logically locate the source of a network failure. ONS 15454 muxponder (MXP) and transponder (TXP) cards used in DWDM configurations allow loopbacks. DWDM cards such as OPT-BST, OPT-PRE, OSC-CSM, and optical add/drop multiplexer cards (band add-drop cards and channel add-drop cards) do not allow loopbacks.

To create a loopback on a port, the port must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. The resulting service state is Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT).

Caution Facility (line) or terminal loopbacks can be service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. Basic directions for these external switching commands exist in Chapter 2, "Alarm Troubleshooting."

Note In Software Release 4.7, loopbacks are not available for DWDM cards.DWDM cards include the OSCM, OSC-CSM,OPT-PRE,OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.xAD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the32WSS.

1.1.1 Facility Loopbacks

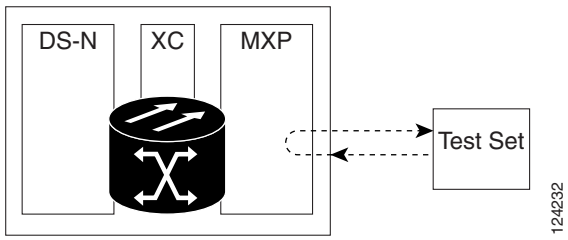
The following sections give general information about facility loopback operations and specific information about ONS 15454 card loopback activity.

1.1.1.1 General Behavior

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

To test an MXP card LIU, connect an optical test set to the MXP port and perform a facility (line) loopback. Or use a loopback on a card that is farther along the circuit path. Figure 1-1 shows a facility loopback on an MXP card.

Figure 1-1 Facility (Line) Loopback Path on a Near-End MXP Card



1.1.1.2 ONS 15454 Card Behavior

ONS 15454 port loopbacks either terminate or bridge the loopback signal. ONS 15454 MXP and TXP facility loopbacks are terminated as shown in Table 1-1.

When a port terminates a facility loopback signal, the signal only loops back to the originating port and is not transmitted downstream. When a port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.

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

Table 1-1 ONS 15454 MXP and TXP Facility Loopback Behavior

Card/Port	Facility loopback signal
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated

MXP, TXP, and FC_MR card facility loopbacks can have different service states for the trunk and client ports. With a client-side facility loopback, the client port service state is Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT); however the remaining client and trunk ports can be in any other service state. For cards in a trunk-side facility loopback, the trunk port service state is OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any other service state.

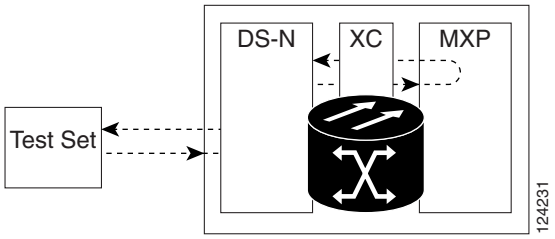
1.1.2 Terminal Loopbacks

The following sections give general information about terminal loopback operations and specific information about ONS 15454 card MXP and TXP loopback activity.

1.1.2.1 General Behavior

A terminal loopback tests a circuit path as it passes through the cross-connect card (XC10G) and loops back from the card with the loopback. Figure 1-2 shows a terminal loopback on an MXP card. The test-set traffic comes into the electrical port and travels through the cross-connect card to the optical card. The terminal loopback on the optical card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the electrical card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the optical card.

Figure 1-2 Terminal Loopback Path on an MXP Card



1.1.2.2 ONS 15454 Card Behavior

ONS 15454 terminal port loopbacks can either terminate or bridge the signal. In ONS 15454 MXP and TXP cards, terminal loopbacks are terminated as shown in Table 1-2. During terminal loopbacks, some ONS 15454 cards bridge the loopback signal while others terminate it.

If a port terminates a terminal loopback signal, the signal only loops back to the originating port and is not transmitted downstream. If the port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.

MXP and TXP card terminal loopback bridging and terminating behaviors are listed in Table 1-2.

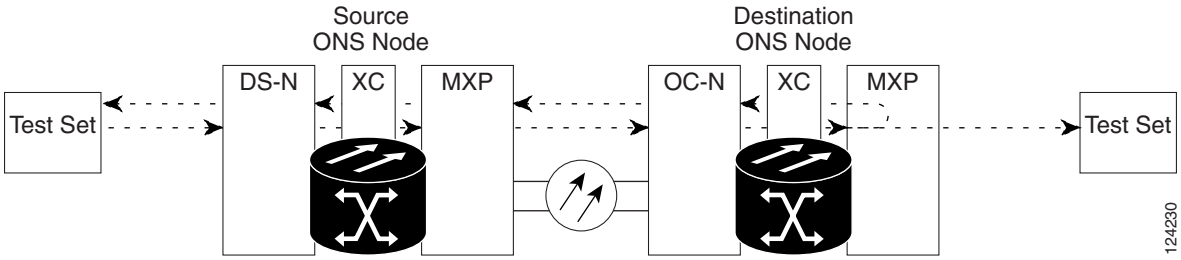
Note In Table 1-2, no AIS signal is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream for all cards except Ethernet cards.

Table 1-2 ONS 15454 MXP Card Terminal Loopback Behavior

Card/Port	Terminal loopback signal
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated

A bridged terminal loopback signal is shown in Figure 1-3.

Figure 1-3 Terminal Loopback on an MXP Card with Bridged Signal



TXP and MXP card trunk and client ports have different service state behaviors and requirements from other ONS 15454 cards. The cards can simultaneously maintain different service states.

- For TXP and TXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and trunk port must be in IS-NR service state.
- For MXP and MXPP cards with a client-side terminal loopback the client port is in the OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any service state.
- In MXP or TXP trunk-side terminal loopbacks, the trunk port is in the OOS-MA,LPBK & MT service state and the client ports must be in IS-NR for complete loopback functionality. A terminal loopback affects all client ports because it is performed on the aggregate signal.

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKTERMINAL condition or LPBKFACILITY condition for a tested port. (The Alarms window will show AS-MT, which indicates that all alarms are suppressed on the port during loopback testing.)

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

- If an electrical or optical port is in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected. For more information about placing ports into alternate states for testing, refer to the *Cisco ONS 15454 Procedure Guide*.

1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks

Facility (line) loopbacks and terminal (inward) loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure. MXP and TXP loopback testing does not require circuit creation (unlike optical, electrical, or Ethernet cards used in SONET and SDH ONS platforms). MXP and TXP client ports are statically mapped to the trunk ports so no signal needs to traverse the cross-connect card (in a circuit) to test the loopback.

The example in this section tests a circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them.

The logical progression contains seven network test procedures:

Note In Software R4.7, loopbacks are not available for DWDM cards. DWDM cards include the OSCM, OSC-CSM,OPT-PRE,OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.xAD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the32WSS.

Note MXP and TXP card client ports do not appear in the Maintenance > Loopback tab unless they have been provisioned. Do this in the card view Provisioning > Pluggable Port Modules tab. For information about provisioning client ports, refer to the *Cisco ONS 15454 Procedure Guide*.

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

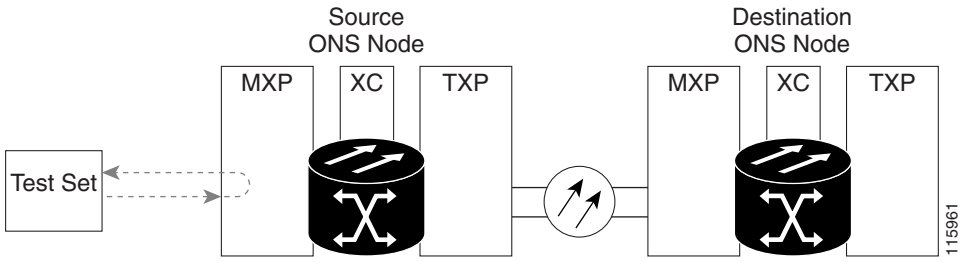
1. A facility (line) loopback on the source-node MXP or TXP port
2. A terminal (inward) loopback on the source-node MXP or TXP port
3. A facility (line) loopback on the intermediate-node MXP or TXP port
4. A terminal (inward) loopback on the intermediate-node MXP or TXP port
5. A facility (line) loopback on the destination-node MXP or TXP port
6. A terminal (inward) loopback on the destination-node MXP or TXP port

Note Facility and terminal loopback tests require on-site personnel.

1.2.1 Perform a Facility (Line) Loopback on a Source-Node MXP or TXP Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the loopback is performed on the source-node muxponder or transponder port. Completing a successful facility (line) loopback on this port isolates the port as a possible failure point. Figure 1-4 shows an example of a facility loopback on a circuit source port.

Figure 1-4 Facility (Line) Loopback on a Circuit Source MXP or TXP Port



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

Complete the "Create the Facility (Line) Loopback on the Source-Node MXP or TXP Port" procedure on page 1-7.

Create the Facility (Line) Loopback on the Source-Node MXP or TXP Port

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

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

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

Step 2 Adjust the test set accordingly.

Step 3 In CTC node view, double-click the card to display the card view.

Step 4 Click the **Maintenance > Loopback** tab.

Step 5 Choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 6 Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 7 Click **Apply**.

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

Note It is normal for a "LPBKFACILITY (OCN)" condition on page 2-159, or a "LPBKFACILITY (G1000)" condition on page 2-157 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the MXP or TXP Facility (Line) Loopback Circuit" procedure on page 1-7.

Test and Clear the MXP or TXP Facility (Line) Loopback Circuit

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

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

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

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

Step 4 Complete the "Create the Terminal (Inward) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-8.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.

d. Click **Apply**.

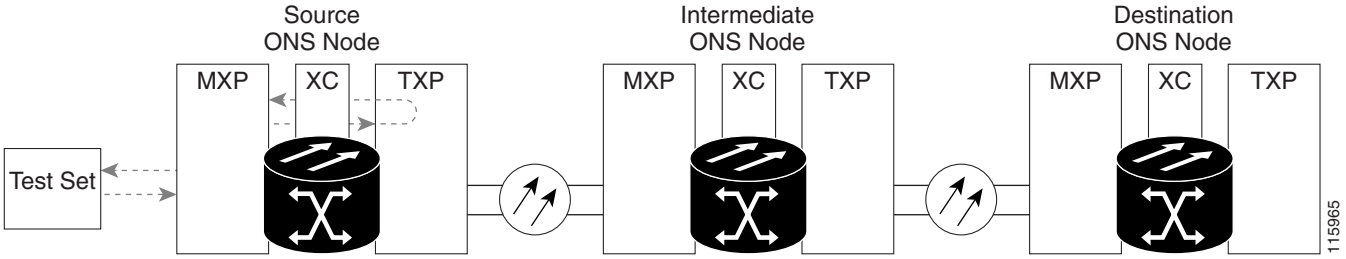
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-8.

1.2.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP or TXP Port

The terminal (inward) loopback test is performed on the node source MXP, TXP, or FC_MR port. For the circuit in this example, it is the source-node MXP port. You first create a bidirectional circuit that starts on the node destination MXP or TXP port and loops back on the node source port.You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-5 shows an example of a terminal loopback on a source port.

Figure 1-5 Terminal (Inward) Loopback on a Source-Node MXP or TXP Port



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

Complete the "Create the Terminal (Inward) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9.

Create the Terminal (Inward) Loopback on a Source-Node MXP or TXP Port

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-6, leave the optical test set hooked up to the source-node MXP or TXP port.

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

Step 2 Adjust the test set accordingly.

Step 3 In node view, double-click the card that requires the loopback, such as the destination OC-N card in the source node.

Step 4 Click the **Maintenance > Loopback** tab.

Step 5 Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

Step 6 Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test and Clear the MXP or TXP Port Terminal Loopback Circuit" procedure on page 1-10.

Test and Clear the MXP or TXP Port Terminal Loopback Circuit

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

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

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

- **a.** Double-click the card in the source node with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-11. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-10.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the defective card.

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

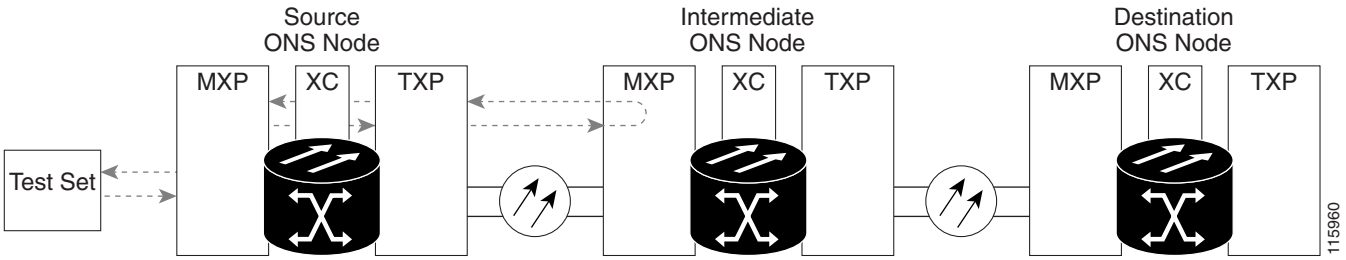
- **a.** Double-click the card in the source node with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-11.

1.2.3 Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-6, the test is being performed on an intermediate MXP or TXP port.

Figure 1-6 Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port



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

Complete the "Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-11.

Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port

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

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

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-8, leave the optical test set hooked up to the source-node port.

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

Step 2 Adjust the test set accordingly.

Step 3 In node view, double-click the intermediate-node card that requires the loopback.

Step 4 Click the **Maintenance > Loopback** tab.

Step 5 Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

Step 6 Select **Facility (Line)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test and Clear the MXP or TXP Port Facility (Line) Loopback Circuit" procedure on page 1-12.

Test and Clear the MXP or TXP Port Facility (Line) Loopback Circuit

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

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

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

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

Step 4 Complete the "Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14. If the test set indicates a faulty circuit, the problem might be a faulty MXP or TXP card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-12.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the faulty card.

Step 5 Clear the facility (line) loopback from the port:

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.

d. Click **Apply**.

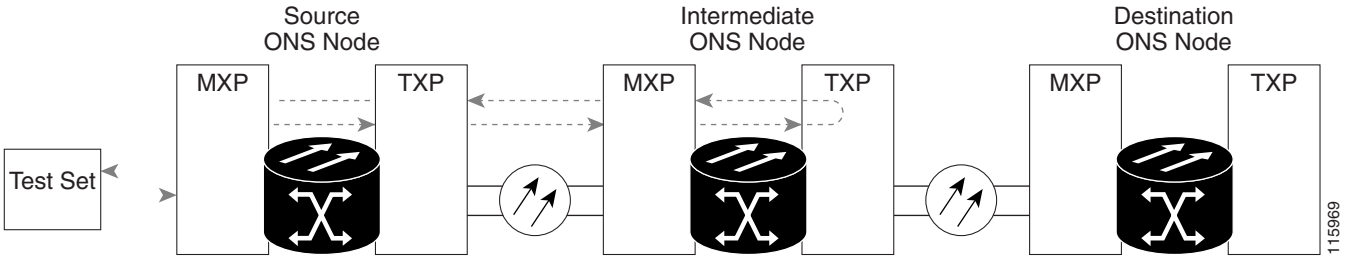
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Create a Terminal (Inward) Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-13.

1.2.4 Create a Terminal (Inward) Loopback on Intermediate-Node MXP or TXP Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-7, the terminal loopback is performed on an intermediate MXP or TXP port in the circuit. You first create a bidirectional circuit that originates on the source-node MXP or TXP port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-7 Terminal Loopback on an Intermediate-Node MXP or TXP Port



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

Complete the "Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14.

Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports

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

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

a. If you just completed the "Create a Facility (Line) Loopback on an Intermediate-Node MXP or TXP Port" section on page 1-11, leave the optical test set hooked up to the source-node port.

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

Step 2 Adjust the test set accordingly.

Step 3 Create the terminal loopback on the destination port being tested:

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

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

b. In node view, double-click the card that requires the loopback.

c. Click the **Maintenance > Loopback** tab.

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

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

f. Click **Apply**.

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

Step 4 Complete the "Test and Clear the MXP or TXP Terminal Loopback Circuit" procedure on page 1-14.

Test and Clear the MXP or TXP Terminal Loopback Circuit

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

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

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

a. Double-click the intermediate-node card with the terminal loopback to display the card view.

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.

e. Click **Apply**.

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

Step 4 Complete the "Create the Facility (Line) Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-16. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-15.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.

e. Click **Apply**.

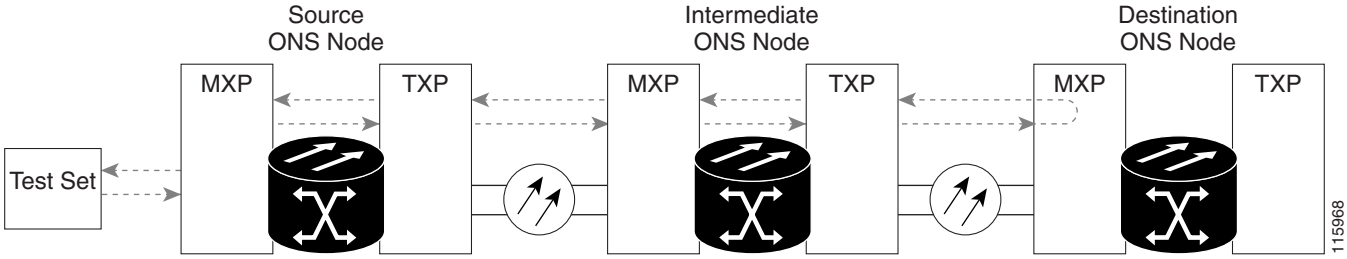
f. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Facility (Line) Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-15.

1.2.5 Perform a Facility (Line) Loopback on a Destination-Node MXP or TXP Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-8 shows a facility loopback being performed on an MXP or TXP port.

Figure 1-8 Facility (Line) Loopback on a Destination-Node MXP or TXP Port



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

Complete the "Create the Facility (Line) Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-16.

Create the Facility (Line) Loopback on a Destination-Node MXP or TXP Port

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

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

a. If you just completed the "Create the Terminal (Inward) Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9, leave the optical test set hooked up to the source-node port.

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

Step 2 Adjust the test set accordingly.

Step 3 Create the facility (line) loopback on the destination port being tested:

a. Go to the node view of the destination node:
   - Choose **View > Go To Other Node** from the menu bar.
   - Choose the node from the pull-down menu in the Select Node dialog box and click **OK**.

b. In node view, double-click the card that requires the loopback.

c. Click the **Maintenance > Loopback** tab.

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

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

f. Click **Apply**.

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

Step 4 Complete the "Test and Clear the MXP or TXP Facility (Line) Loopback Circuit" procedure on page 1-17.

Test and Clear the MXP or TXP Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Create the Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-18. If the test set indicates a faulty circuit, the problem might be a faulty MXP or TXP card.

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-17.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the faulty card.

Step 5 Clear the facility (line) loopback on the port:

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) from the Admin State column for the port being tested.

d. Click **Apply**.

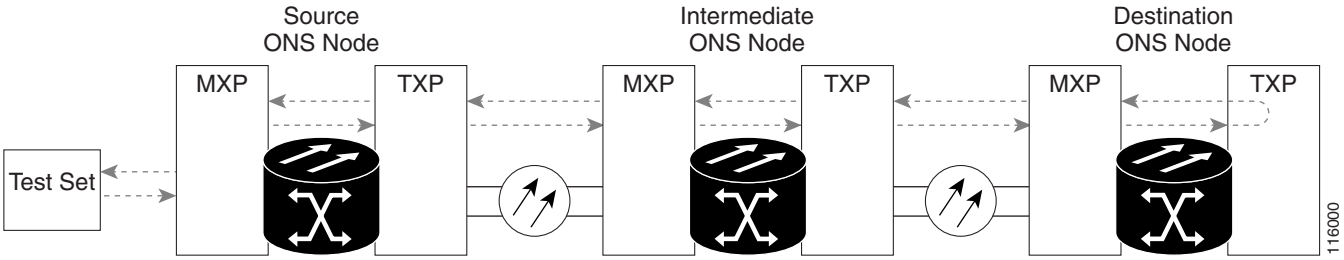
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-18.

1.2.6 Perform a Terminal Loopback on a Destination-Node MXP or TXP Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-9 shows a terminal loopback on an intermediate-node destination MXP or TXP port.

Figure 1-9 Terminal Loopback on a Destination-Node MXP or TXP port



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

Complete the "Create the Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-18.

Create the Terminal Loopback on a Destination-Node MXP or TXP Port

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-15, leave the optical test set hooked up to the source port.

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

Step 2 Adjust the test set accordingly.

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

Note It is normal for the "LPBKTERMINAL (OCN)" condition on page 2-163 to appear during a loopback setup. The condition clears when you remove the loopback.

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

a. Go to the node view of the destination node:
   - Choose **View > Go To Other Node** from the menu bar.
   - Choose the node from the pull-down menu in the Select Node dialog box and click **OK**.

b. In node view, double-click the card that requires the loopback.

c. Click the **Maintenance > Loopback** tab.

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the MXP or TXP Terminal Loopback Circuit" procedure on page 1-19.

Test and Clear the MXP or TXP Terminal Loopback Circuit

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

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

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

a. Double-click the intermediate-node card with the terminal loopback.

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.

e. Click **Apply**.

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

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

Step 5 Complete the "Test the MXP or TXP Card" procedure on page 1-20.

Test the MXP or TXP Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the suspected bad card and replace it 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. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

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

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

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT; IS,AINS) in the State column for the port being tested.

e. Click **Apply**.

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

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

1.3 Troubleshooting DWDM Circuit Paths With G.709 Monitoring

This section provides an overview of the optical transport network (OTN) specified in ITU-T G.709 Network Node Interface for the Optical Transport Network, and provides troubleshooting procedures for DWDM circuit paths in the G.709 OTN using performance monitoring and threshold crossing alerts (TCAs).

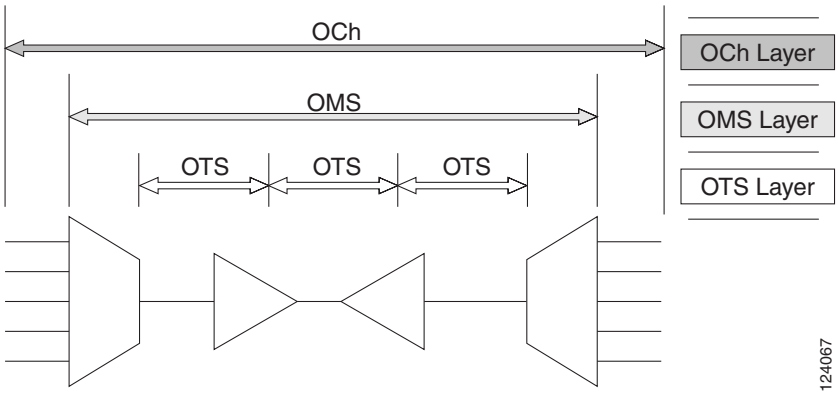
1.3.1 G.709 Monitoring in Optical Transport Networks

Recommendation G.709 is part of a suite of recommendations covering the full functionality of an OTN. G.709 takes single-wavelength SONET technology a step further by enabling transparent optical wavelength-based networks. It adds extra overhead to existing SONET, Ethernet, or ATM bit streams for performance management and improvement.

G.709 adds the operations, administration, maintenance and provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks.

Like traditional SONET networks, G.709 optical networks have a layered design (Figure 1-10). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 1-10 Optical Transport Network Layers



1.3.2 Optical Channel Layer

The optical channel (OCh) layer is the outermost part of the OTN and spans from client to client. The optical channel is built as follows:

1. A client signal such as SONET, Gigabit Ethernet, IP, asynchronous transfer mode (ATM), fiber channel, or enterprise system connection (ESCON) is mapped to a client payload area and combined with an overhead to create the optical channel payload unit (OPUk).
2. A second overhead is added to the OPUk unit to create the optical channel data unit (ODUk).
3. A third overhead including forward error correction (FEC) is added to the ODUk to create the optical channel transport unit (OTUk).
4. A fourth overhead is added to the OTUk to create the entire OCh layer

1.3.3 Optical Multiplex Section Layer

The optical multiplex section (OMS) of the OTN allows carriers to identify errors occurring within DWDM network sections. The OMS layer consists of a payload and an overhead (OMS-OH). It supports the ability to monitor multiplexed sections of the network, for example the span between an optical multiplexer such as the 3 2MUX-O and a demultiplexer such as the 32 DMX-O.

1.3.4 Optical Transmission Section Layer

The optical transmission section (OTS) layer supports monitoring partial spans of a network's multiplexed sections. This layer consists of a payload and an overhead (OTS-OH). It is a transmission span between two elements in an optical network, such as between:

- a multiplexer such as the 32 MUX-O and an amplifier such as the OPT-PRE;
- an amplifier and another amplifier, such as the OPT-BST and the OPT-PRE;
- or an amplifier such as the OPT-BST and a demultiplexer such as the 32-DMX.

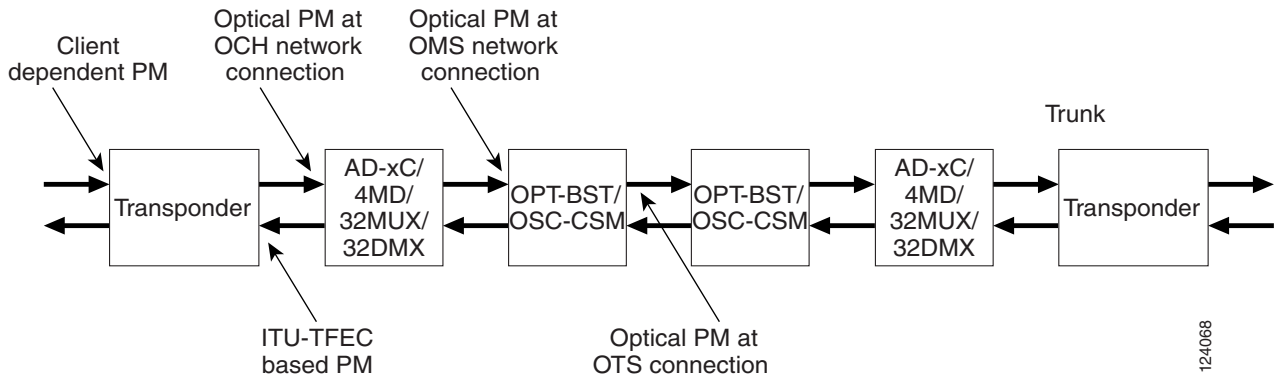
1.3.5 Performance Monitoring Counters and Threshold Crossing Alerts

Performance monitoring (PM) counters and TCAs can be used for identifying trouble and troubleshooting problems in G.709 optical transport networks. ITU-T Recommendation M.2401 recommends that the following PM parameters be monitored at the ODUk Layer:

- SES (severely errored seconds)—A one-second period which contains greater than or equal to 30% errored blocks or at least one defect. SES is a subset of the errored second (ES) parameter, which is a on- second period with one or more errored blocks or at least one defect.
- BBE (background block error counter)—An errored block not occurring as part of an SES. BBE is a subset of the errored block (EB) parameter, which is a block in which one or more bits are in error.

Different performance monitoring count parameters are associated with different read points in a network. Figure 1-11 illustrates the performance monitoring read points that are useful in identifying DWDM circuit points of failure. Chapter 4, "Performance Monitoring," lists all PM parameters and provides block diagrams of signal entry points, exit points and interconnections between the individual circuit cards. Consult these specifications to determine which performance monitoring parameters are associated with the system points you want to monitor or provision with CTC or TL1. The monitoring points can vary according to your configuration.

Figure 1-11 Performance Monitoring Points on ONS DWDM



TCAs are used to monitor performance through the management interface by indicating whether preset thresholds have been crossed, or whether a transmission (such as a laser transmission) is degraded. TCAs are not associated with severity levels. They are usually associated with rate, counter, and percentage parameters that are available at transponder monitoring points. Chapter 4, "Performance Monitoring," contains more information about these alerts.

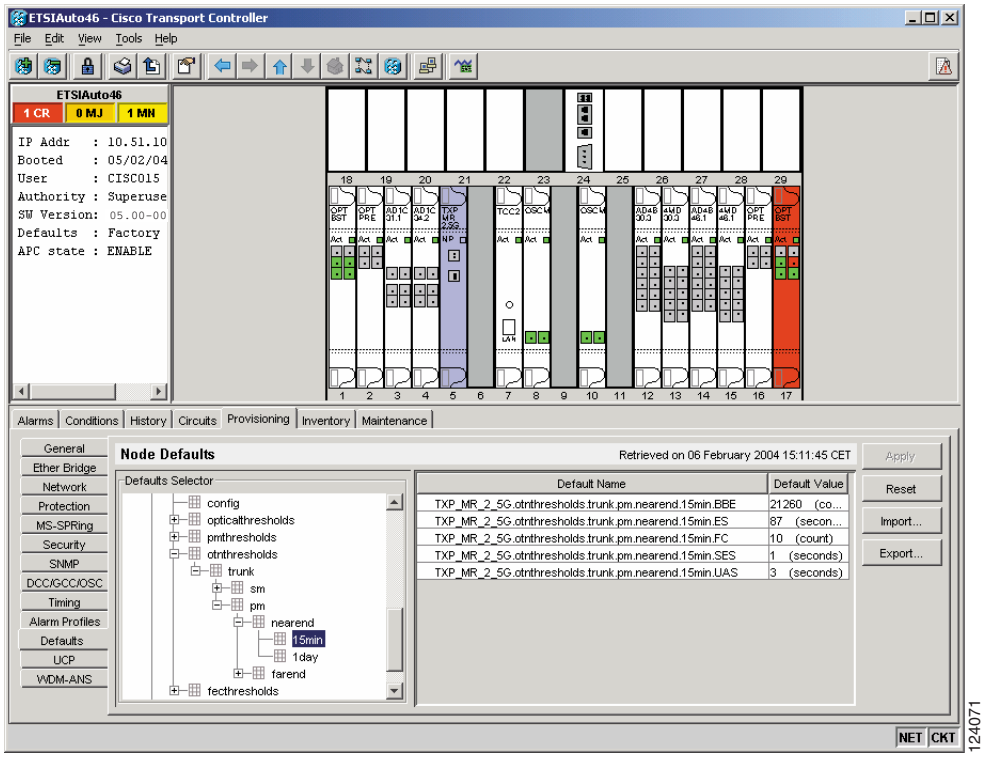
Select and complete the provisioning procedure below according to your network parameters.

Complete the following procedure to provision default node ODUk BBE and SES PM thresholds for TXP cards.

Set Node Default BBE or SES Card Thresholds

Step 1 In node view, click the **Provisioning > Defaults** tabs (Figure 1-12).

Figure 1-12 Set Default BBE/SES Card Thresholds



Step 2 In the Defaults Selector field, select Txp_mr_2_5g > otnthresholds > Trunk > pm > 15min.

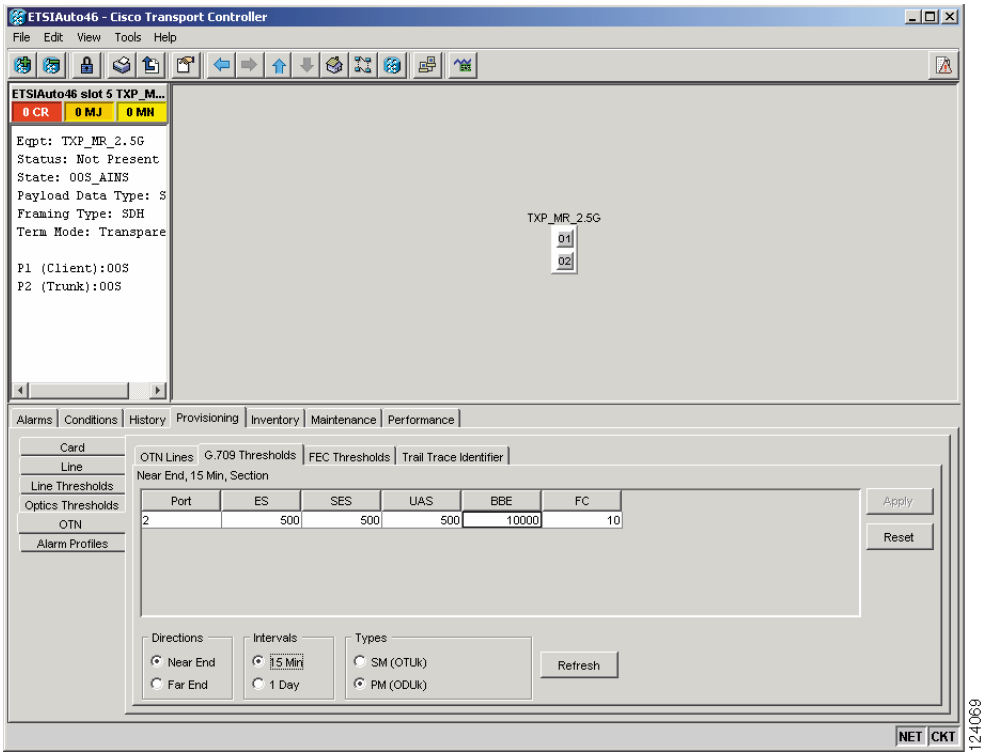
Complete the following procedure to provision BBE or SES PM thresholds in CTC for an individual TXP card.

Provision Individual Card BBE or SES Thresholds in CTC

Step 1 In node view, double-click the TXP_MR_2.5G card.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning** > **OTN** > **G.709 Thresholds** tabs (Figure 1-13).

Figure 1-13 Provision Card BBE/SES Thresholds



Step 3 In the Directions area, click **Near End**.

Step 4 In the Intervals area, click **15 Min**.

Step 5 In the Types area, click **PM (ODUk)**.

Step 6 In the SES and BBE fields, enter threshold numbers, for example 500 and 10000.

Complete the following procedure if you wish to provision PM thresholds in TL1 rather than in CTC.

Provision Card PM Thresholds Using TL1

Step 1 Open a TL1 command line.

Step 2 On the TL1 command line, use the following syntax:

```
set-th-{och,clnt}::aid:ctag::montype,thlev,,,[tmper];
```

Where:

- The modifier is och, as applicable to the trunk port.
- Montype can be:
  - BBE-PM
  - SES-PM
  - LBCL-MAX

- The thlev parameter is optional and indicates a threshold count value, which is the number of errors which must be exceeded before the threshold is crossed.
- The tmper parameter is optional and is an accumulation time period for performance counters, with possible values of 1-DAY, 1-HR, 1-MIN, 15-MIN, and RAW-DATA.

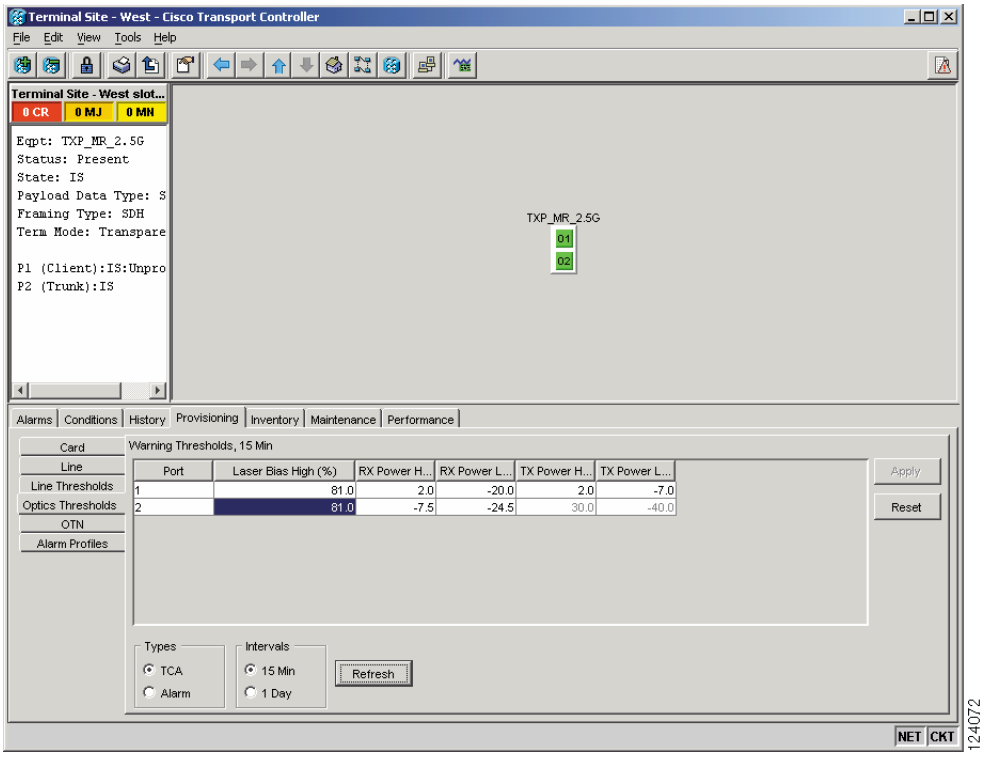
Note For a list of TL1 commands, refer to the *Cisco ONS 15454 SONET and SDH TL1 Quick Reference Guide, Release 4.7*.

Complete the following procedure to provision TCA thresholds in CTC.

Provision Optical TCA Thresholds

Step 1 In node view, click the **Provisioning > Optics Thresholds** tabs (Figure 1-14).

Figure 1-14 Provision Optical TCA Thresholds



Step 2 In the Types area, click **TCA**.

Step 3 In the Intervals area, click **15 Min**.

Step 4 In the Laser Bias High (%) field, enter the threshold value, for example, 81.0 percent.

1.3.6 Forward Error Correction

In DWDM spans, FEC reduces the quantities of 3R regeneration needed to maintain signal quality. The following two PM parameters are associated with FEC:

- BIEC—Bit errors corrected (BIEC) indicates the number of bit errors corrected in the DWDM trunk line during the PM time interval.
- UNC-WORDS—The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

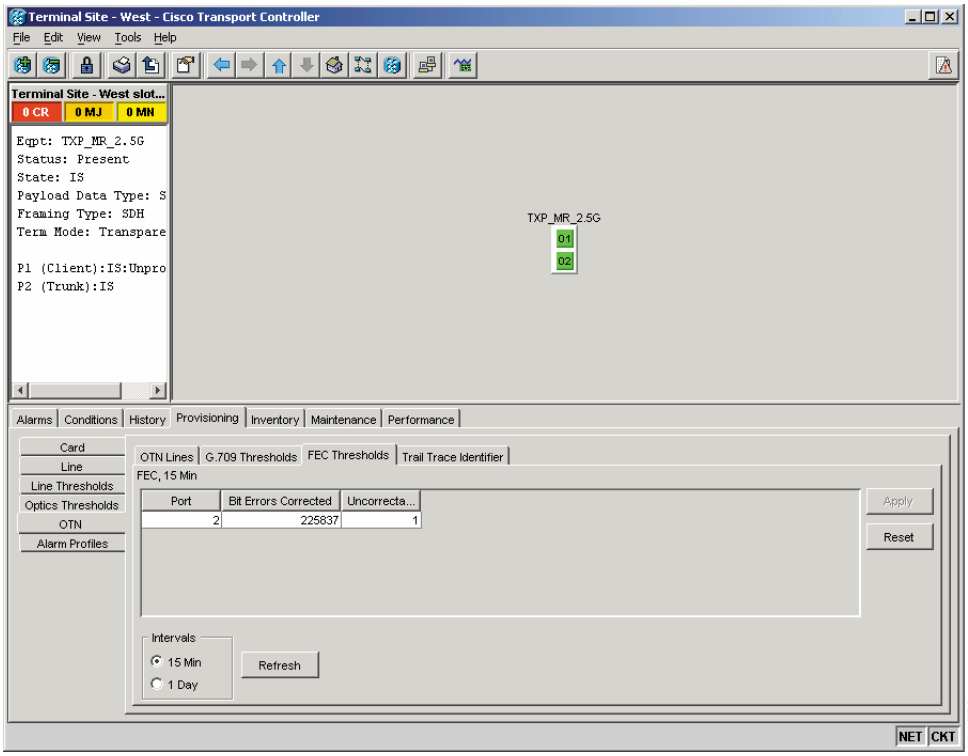
Complete the following procedure to provision BIEC and UNC-WORDS PM parameters for FEC.

Provision Card FEC Thresholds

Step 1 In node view, double-click the TXP_MR_2.5G card to open the card view.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning > OTN > FEC Thresholds** tabs (Figure 1-15).

Figure 1-15 Provisioning Card FEC Thresholds



Step 3 In the Bit Errors Corrected field, enter a threshold number, for example 225837.

Step 4 In the Intervals area, click **15 Min**.

1.3.7 Sample Trouble Resolutions

Some sample trouble resolutions using performance monitoring and TCAs for isolating points of degrade are provided below.

Symptom There is a BBE TCA on a single transponder pair.

Possible Cause The transponder input power is out of range.

Recommended Action Check the input power on the transponder. It should be within the specified/supported range.

Possible Cause There are dirty trunk connectors on the transponder.

Recommended Action Check the connector on the trunk port.

Possible Cause There is a degraded trunk patch-cord between the transponder and the DWDM port.

Recommended Action Check the patch-cord on the transponder DWDM port.

Possible Cause There are dirty client connectors on the channel add-drop (ADxC transmit port or the demultiplexer (DMX) has crossed the near-end TCA.

Recommended Action Check the connector on the OCH port of the ADxC.

Possible Cause There are dirty client connectors on the ADxC receive port or the multiplexer (MUX) has crossed the far-end TCA point.

Recommended Action If an optical channel bypass exists along the line, check the connectors.

Symptom There is a BBE TCA on all transponders connected to a band add-drop card (ADxB).

Possible Cause The transponder input power is out of range.

Recommended Action Check the input power on the transponder. It should be within the specified/supported range.

Possible Cause There is a dirty connector on the 4MD port.

Recommended Action Check the connector on the drop port of the ADxB.

Possible Cause There is a dirty connector on the ADxB drop port -and it has crossed the near-end TCA point.

Recommended Action Check the connector on the drop port of the 4MD.

Possible Cause There is a dirty connector on the ADxB add port and it has crossed the far-end TCA.

Recommended Action Check the patch-cord on the 4MD or AD1Bx.

Possible Cause There is a degraded patch-cord between the ADxB and the 4MD.

Recommended Action If an optical band bypass exists along the line, check the band connectors.

Symptom There is a BBE TCA on all transponders which the OCH passes through a single OTS section.

Possible Cause This is not a transponder or channel- related issue.

Recommended Action The problem is in the intercabinet signal path preceding the transponder. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about configurations and acceptance tests for this area

Symptom You have an LBC TCA on a single transponder.

Possible Cause The laser of the transponder is degrading.

Recommended Action The problem is within the laser circuitry. Check the OPT-PRE or OPT-BST optical amplifier cards. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about setting up these cards.

1.4 Using CTC Diagnostics

In Release 4.7, CTC provides diagnostics for the following functions:

- Verify that card LEDs operate properly.
- Verify that the ASICs on all cards are working.
- Verify the Standby cards are able to handle traffic should a switchover occur.
- Notify the customer of any problems detected via alarms.
- Verify the protection path of a BLSR is operational.

Some of these functions, such as ASIC verification and standby card operation, are invisibly monitored in background functions. Change or problem notifications are provided in the Alarms and Conditions window. Other diagnostic functions—verifying card LED function, creating BLSR diagnostic circuits, and also downloading diagnostic files for technical support—are available to the user in the node view Maintenance > Diagnostic tab. The user-operated diagnostic features are described in the following paragraphs.

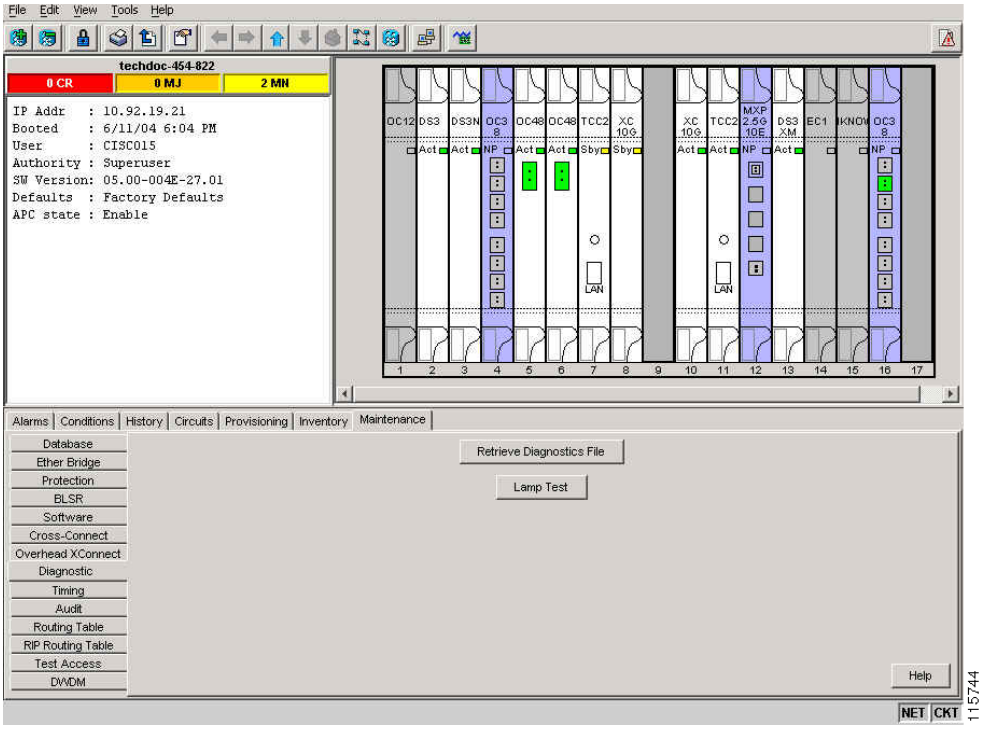
1.4.1 Card LED Lamp Tests

A card LED lamp test determines whether card-level indication LEDs are operational. This diagnostic test is run as part of the initial ONS 15454 turnup, during maintenance routines, or any time you question whether an LED is in working order. Maintenance or higher-level users can complete the following tasks to verify LED operation.

Verify General Card LED Operation

Step 1 In node view, click the **Maintenance > Diagnostic** tab (Figure 1-16).

Figure 1-16 CTC Diagnostic Window



Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate simultaneously for several seconds.

Step 4 Click **OK** on the Lamp Test Run dialog box.

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

1.4.2 Retrieve Diagnostics File Button

When you click the Retrieve Diagnostics File button in the Maintenance window, CTC retrieves system data that can be off-loaded by a Maintenance or higher-level user to a local directory and sent to Technical Support for troubleshooting purposes. The diagnostics file is in machine language and is not human-readable, but can be used by Cisco Technical Support for problem analysis. Complete the following task to off-load the diagnostics file.

Note In addition to the machine-readable diagnostics file, the ONS 15454 also stores an audit trail of all system events such as user logins, remote logins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Off-Load the Diagnostics File

Step 1 In the node view, click the **Maintenance > Diagnostic** tab (Figure 1-16).

Step 2 Click **Retrieve Diagnostics File**.

Step 3 In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.

Step 4 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 5 Click **Save**.

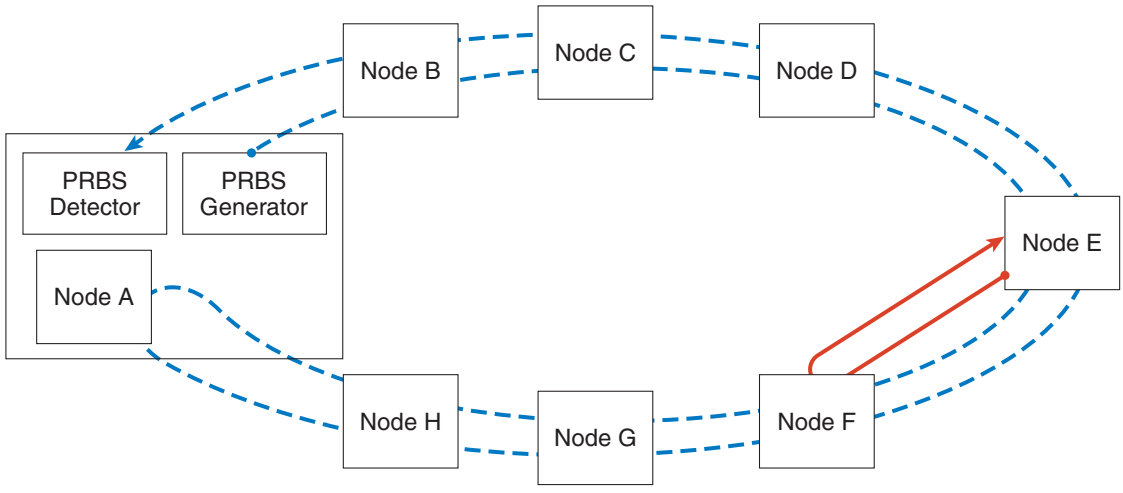
The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows "Get Diagnostics Complete."

Step 6 Click **OK**.

1.4.3 BLSR Diagnostic Circuit

In Release 5.0, CTC provides a diagnostic BLSR loopback circuit feature that uses pseudo-random bit sequence (PRBS) error detection to monitor standby circuit path readiness. The diagnostic circuit originates and terminates on a single node, where the signal result is detected and analyzed for errors. The circuit can be configured for an end-to-end or multiple-node path layout, traversing the transmit and receive standby paths as shown in Figure 1-17.

Figure 1-17 CTC Node View Diagnostic Window



Each card type utilizes the diagnostic feature differently. Standby electrical cards run PRBS tests to ensure signal path integrity. Optical cards do not run PRBS tests, but instead run ASIC tests to test card operability. Cross-connect cards verify the standby BLSR paths.

A diagnostic BLSR circuit is created much the same way as a normal standby PCA circuit but is designated by checking the Diagnostic checkbox during circuit creation. A normal circuit uses line cards as the endpoints, but if a circuit is configured as a diagnostic the endpoints are cross-connect cards.

In Release 5.0, the maximum diagnostic circuit size is VT1.5. The circuit can only be created if the same STS is available on each span the circuit traverses. Only one BLSR diagnostic circuit can be sourced and detected per node. When you use a BLSR diagnostic that traverses one or more intermediate nodes, create or utilize an existing bidirectional circuit on each intermediate node. At the terminating node, you will need to create a

Create a BLSR Diagnostic Circuit

Step 1 Log into the node where you will create the diagnostic circuit.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, refer to the task for assigning a name to a port in the *Cisco ONS 15454 Procedure Guide*. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

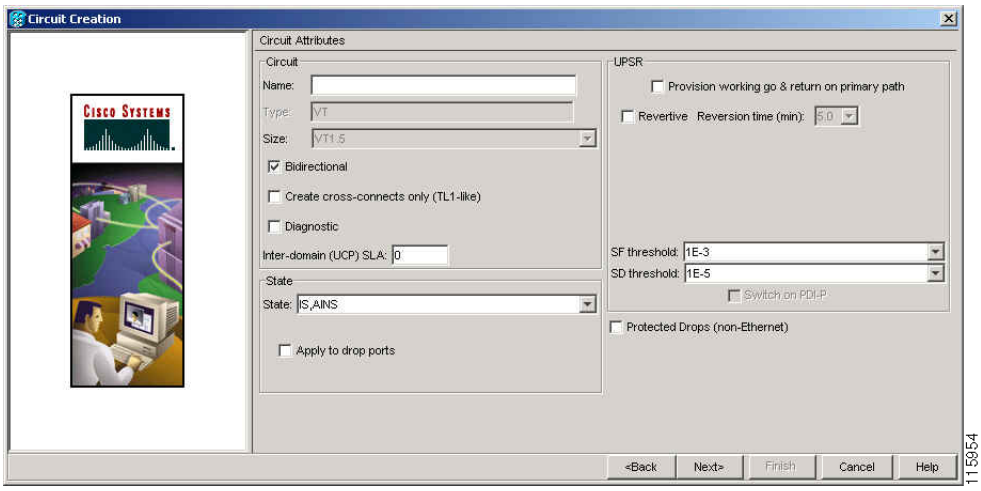
Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT**.
- Number of Circuits—Type the number of circuits you want to create. The default is 1.
- Auto-ranged—Uncheck the box.

Step 6 Click **Next**.

Step 7 Define the circuit attributes in the Circuit Creation Dialog Box shown in Figure 1-18 using the following parameters:

Figure 1-18 Network View Circuit Creation Dialog Box



- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—This is the default value. Leave it checked for this circuit.
- State—Choose the administrative state to apply to all of the cross-connects in a circuit:
  - IS—Places the circuit cross-connects in the IS-NR service state.
  - OOS,DSBLD—Places the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Places the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Places the circuit cross-connects in the OOS-MA,MT service state. This service state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. For instructions and information about administrative and service states, refer to the *Cisco ONS 15454 Procedure Guide*.

Note If VT circuit source and destination ports are in an OOS-AU,AINS; OOS-MA,MT; or IS-NR service state, VT circuit connections in OOS-AU,AINS change to IS-NR even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

- Diagnostic—Check this box to create a diagnostic circuit.
- Apply to drop ports—Check this box if you want to apply the service state chosen in the State field to the circuit source and destination ports. If the box is unchecked, CTC does not change the state of the source and destination ports. The circuit bandwidth is the same as the port bandwidth. If the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. For the requirements necessary to apply a service state to drop ports, refer to the *Cisco ONS 15454 Reference Manual*.

Note LOS alarms are generated if in service (IS-NR) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Disabled for a diagnostic circuit.
- Inter-domain (UCP) SLA—Disabled for a diagnostic circuit.
- Protected Drops—Disabled for a diagnostic circuit.

Step 8 Click **Next**.

Step 9 In the Source area of the Circuit Creation pane, complete the following:

a. From the Node pull-down menu, choose the node.

b. From the Slot pull-down menu, choose **PRBS Generator**.

c. Click **Next**.

Step 10 In the Destination area of the Circuit Creation pane, complete the following:

a. From the Node pull-down menu, choose the node. The only selectable item in the list is the node chosen as the source node.

b. From the Slot pull-down menu, choose the slot where the BLSR span originates.

c. From the STS pull-down menu, choose the STS.

d. From the VT pull-down menu, choose the VT.

e. Click **Next**.

Step 11 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 10 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 12 In the Circuits window, verify that the new circuit(s) appear in the circuits list.

1.5 Restoring the Database and Default Settings

This section contains troubleshooting for node operation errors that require restoration of software data or the default node setup.

1.5.1 Restore the Node Database

Symptom One or more nodes are not functioning properly or have incorrect data.

Possible Cause There is an incorrect or corrupted node database.

Recommended Action Perform a Restore the Database procedure. Refer to the "Restore the Database" procedure on page 1-33.

Restore the Database

Caution E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The "CARLOSS (E100T, E1000F)" alarm on page 2-46 appears and clears during this period.

Caution If you are restoring the database on multiple nodes, wait approximately one minute after the TCC2 reboot has completed on each node before proceeding to the next node

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

Step 1 In CTC, log into the node where you will restore the database:

a. On the PC connected to the ONS 15454, start Netscape or Internet Explorer.

b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box appears.

c. In the Login dialog box, type a user name and password (both are case sensitive) and click **Login**. The CTC node view window appears.

Step 2 Ensure that no ring or span (four-fiber only) switch events are present; for example, ring-switch east or west and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve** to view a list of conditions.

Step 3 If switch events need to be cleared, in node view click the **Maintenance > BLSR** tab and view the West Switch and East Switch columns.

a. If a switch event (not caused by a line failure) is present, choose **CLEAR** from the pull-down menu and click **Apply**.

b. If a switch event caused by the Wait to Restore (WTR) condition is present, choose **LOCKOUT SPAN** from the pull-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the pull-down menu and click **Apply**.

Step 4 In node view, click the **Maintenance > Database** tab.

Step 5 Click **Restore**.

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

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15454 software CD.

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup might affect traffic on the login node.

Step 9 Click **Yes**.

The Restore Database dialog box monitors the file transfer.

Step 10 Wait for the file to complete the transfer to the TCC2.

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

Step 12 If you cleared a switch in Step 3, reapply the switch as needed.

1.5.2 Restore the Node to Factory Configuration

Symptom A node has both TCC2 cards in standby state, and you are unable reset the TCC2 cards to make the node functional.

Possible Cause Both TCC2 cards are failing in the node.

Possible Cause You are replacing both TCC2 cards at the same time.

Recommended Action Restore the node to factory configuration. Refer to the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-36 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-37 as required.

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

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution If you are restoring the database on multiple nodes, wait until the TCC2 cards have rebooted on each node before proceeding to the next node.

Caution Restoring a node to factory configuration on a Windows or UNIX workstation should only be carried out on a standby TCC2 card.

Caution Cisco recommends that you take care to save the node database to a safe location if you will not be restoring the node using the database provided on the software CD.

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

Note If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-19 on page 1-36).

Note If you need to install or replace one or more TCC2 cards, refer to the *Cisco ONS 15454 Procedure Guide* for installation instructions.

Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Restoring a node to factory configuration on a Windows workstation should only be carried out on a standby TCC2 card.

Note The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

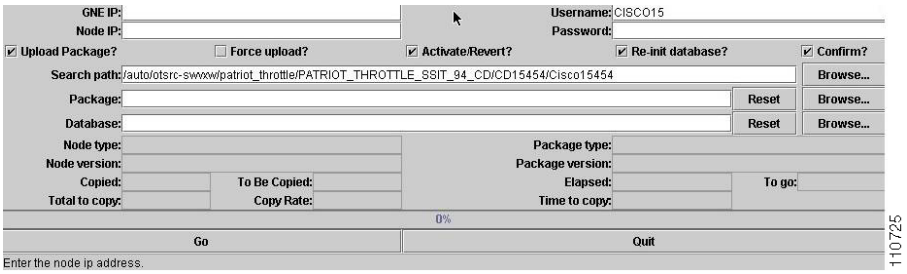
Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.

Step 3 On the CD drive, go to the CISCO15454 folder and choose **All Files from the Files of Type** pull-down menu.

Step 4 Select the RE-INIT.jar file and click **Open** to open the reinit tool (Figure 1-19).

Figure 1-19 Reinitialization Tool in Windows



Step 5 If the node you are reinitializing is an end network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

Step 6 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-19).

Step 7 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 8 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 9 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.7 when version 4.7 is already active), check the Force Upload checkbox.This option forces the NE to have the same software version on the working and protect flash memory.

Note The Force Upload box is only applicable when the Upload Package checkbox is checked.

Step 10 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

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

Step 11 Click **Go**. A confirmation dialog box appears.

Step 12 Click **Yes**.

Step 13 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC2 successfully uploaded the database, not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

Step 14 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC2 card or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

Step 15 Manually set the node name and network configuration to site-specific values. See the *Cisco ONS 15454 DWDM Installation and Operations Guide* for information about setting the node name, IP address, mask and gateway, and IIOP port.

Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Caution Restoring a node to the factory configuration deletes all cross-connects on the node.

Caution Restoring a node to factory configuration on a UNIX workstation should only be carried out on a standby TCC2 card.

Note The TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

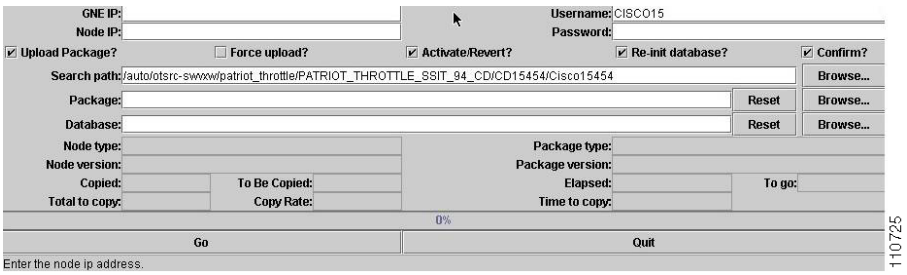
Note Java Runtime Environment (JRE) 1.03_02 must also be installed on the computer you use to perform this procedure.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454).

Step 3 If you are using a file explorer, double-click the **RE-INIT.jar** file to open the reinit tool (Figure 1-20). If you are working with a command line interface, run **java -jar RE-INIT.jar**.

Figure 1-20 Reinitialization Tool in UNIX



Step 4 If the node you are reinitializing is an ENE in a proxy server network, enter the IP address of the GNE in the GNE IP field. If not, leave it blank.

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-20).

Step 6 If the User ID field does not contain your user ID, enter the ID. Enter your password in the Password field.

Step 7 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, check the check box.

Step 8 If you are uploading the same version of software that is already active (for example, you are trying to upload version 4.7 when version 4.7 is already active), check the Force Upload checkbox. This option forces the NE to have the same software version on the working and protect flash memory.

Step 9 In the Search Path field, verify that the path to the CISCO15454 folder on the CD-ROM drive is listed.

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

Step 10 Click **Go**. A confirmation dialog box appears.

Step 11 Click **Yes**.

Step 12 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC2 successfully uploaded the database; not that the database restore was successful. The TCC2 then tries to restore the database after it reboots.

Step 13 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC2 card or on the hub or switch where the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

Step 14 Set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedure Guide* for information about provisioning the node name, IP address, subnet mask and gateway, and IIOP port.

1.6 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R4.7, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.6.1 PC System Minimum Requirements

Workstations running CTC R4.7 for the ONS products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space
- 20 GB or larger hard drive

1.6.2 Sun System Minimum Requirements

Workstations running CTC R4.7 for the ONS products on Sun workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 Mb or more of RAM
- 50 Mb or more of available hard disk space

1.6.3 Supported Platforms, Browsers, and JREs

Software R4.7 CTC supports the following platforms:

- Windows NT
- Windows 98
- Windows XP
- Windows 2000
- Solaris 8
- Solaris 9

Software R4.7 CTC supports the following browsers and JREs:

- Netscape 4.76 (on Solaris 8 or 9 with Java plug-in 1.3.1)
- Netscape 7 (on Solaris 8 or 9 with Java plug-in 1.4)

- PC platforms with Java plug-in 1.3.1 or 1.4
- Internet Explorer 6.0 (on PC platforms with Java plug-in 1.3.1 or 1.4)

Note You can obtain browsers at the following URLs:
Netscape: http://channels.netscape.com/ns/browsers/default.jsp
Internet Explorer: http://www.microsoft.com

Note The recommended JRE version is JRE 1.4.2.

Note JRE 1.4.2 for Windows and Solaris is available on R4.7 product CDs.

1.6.4 Unsupported Platforms and Browsers

Software R4.7 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R4.7 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris is not supported except when used with JRE 1.3.1.
- JRE 1.4.2 is not supported except with Netscape 7 on Solaris 8 or 9.

1.6.5 Unable to Verify the IP Configuration of Your PC

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

Possible Cause The IP address was typed incorrectly.

Recommended Action Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. See the "Verify the IP Configuration of Your PC" procedure on page 1-41.

Possible Cause The IP configuration of your PC is not properly set.

Recommended Action Verify the IP configuration of your PC. Complete the "Verify the IP Configuration of Your PC" procedure on page 1-41. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

Step 1 Open a DOS command window by selecting **Start > Run** from the Start menu.

Step 2 In the Open field, type **command** and then click **OK**. The DOS command window appears.

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

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

The Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.

Note The winipcfg command only returns the information above if you are on a network.

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

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

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

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

1.6.6 Browser Login Does Not Launch Java

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

Possible Cause The PC operating system and browser are not properly configured.

Recommended Action Reconfigure the PC operating system java plug-in control panel and the browser settings. Complete the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-41 and the "Reconfigure the Browser" procedure on page 1-42.

Reconfigure the PC Operating System Java Plug-in Control Panel

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

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

a. Run the Cisco ONS 15454 software CD.

b. Open the *CD-drive:*\Windows\JRE folder.

c. Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.

d. Follow the JRE installation wizard steps.

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

Step 4 In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.

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

Step 6 Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

Step 7 Select **JRE 1.4**.

Step 8 Click **Apply**.

Step 9 Close the Java Plug-in Control Panel window.

Reconfigure the Browser

Step 1 From the Start Menu, launch your browser application.

Step 2 If you are using Netscape Navigator:

a. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

b. In the Preferences window, click the **Advanced > Proxies** categories.

c. In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.

d. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

e. In the Preferences window, click the **Advanced > Cache** categories.

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Windows 98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**
- For Windows NT/2000, **C:\ProgramFiles\Netscape***username***\Communicator\cache**.

g. If the Disk Cache Folder field is not correct, click **Choose Folder**.

h. Navigate to the file listed in Step f, and click **OK**.

i. Click **OK** on the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

a. On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

b. In the Internet Options window, click the **Advanced** tab.

c. In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for** *applet* **(requires restart)** check box.

d. Click **OK** in the Internet Options window and exit the browser.

Step 4 Temporarily disable any virus-scanning software on the computer. See the "Browser Stalls When Downloading CTC JAR Files From TCC2" section on page 1-47.

Step 5 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 6 Restart the browser and log on to the ONS 15454.

1.6.7 Unable to Verify the NIC Connection on Your PC

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

Possible Cause The CAT-5 cable is not plugged in properly.

Recommended Action Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.

Possible Cause The CAT-5 cable is damaged.

Recommended Action Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending.

Possible Cause Incorrect type of CAT-5 cable is being used.

Recommended Action If connecting an ONS 15454 directly to your laptop, a PC, or a router, use a straight-through CAT-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of CAT-5 cables, see the "Crimp Replacement LAN Cables" section on page 1-65.

Possible Cause The NIC is improperly inserted or installed.

Recommended Action If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. (If the NIC is built into the laptop or PC, verify that the NIC is not faulty.)

Possible Cause The NIC is faulty.

Recommended Action Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting a to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.6.8 Verify PC Connection to the ONS 15454 (ping)

Symptom The TCP/IP connection was established and then lost.

Possible Cause A lost connection between the PC and the ONS 15454.

Recommended Action Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2 card. A ping command should work if the PC connects directly to the TCC2 card or uses a LAN to access the TCC2 card. Complete the "Ping the ONS 15454" procedure on page 1-44.

Ping the ONS 15454

Step 1 Display the command prompt:

a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type **command** in the Open field of the Run dialog box, and click **OK**.

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

Step 2 For both the Sun and Microsoft operating systems, at the prompt type:

```
ping ONS-15454-IP-address
```

For example:

```
ping 198.168.10.10
```

Step 3 If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 4 If the ping is successful, an active TCP/IP connection exists. Restart CTC.

Step 5 If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation's IP address is on the same subnet as the ONS node.

Step 6 If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation's NIC is illuminated.

1.6.9 Unknown Node IP Address

Symptom The IP address of the node is unknown and you are unable to login.

Possible Cause The node is not set to the default IP address.

Recommended Action Leave one TCC2 card in the shelf. Connect a PC directly to the remaining TCC2 card and perform a hardware reset of the card. The TCC2 card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the "Retrieve Unknown Node IP Address" procedure on page 1-44.

Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active TCC2 card Ethernet port on the faceplate.

Step 2 Start the Sniffer application on your PC.

Step 3 Perform a hardware reset by pulling and reseating the active TCC2 card.

Step 4 After the TCC2 card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.

1.7 CTC Operation Troubleshooting

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

1.7.1 CTC Colors Do Not Appear Correctly on a UNIX Workstation

Symptom When running CTC on a UNIX workstation, the colors do not appear correctly. For example, both major and minor alarms appear in the same color.

Possible Cause When running in 256-color mode on a UNIX workstation, color-intensive applications such as Netscape might use all of the colors.

Recommended Action CTC requires a full 24-color palette to run properly. When logging into CTC on a UNIX workstation, run as many colors as your adapter will support. In addition, you can use the -install or the -ncols 32 command line options to limit the number of colors that Netscape uses. Complete the "Limit Netscape Colors" procedure on page 1-45. If the problem persists after limiting Netscape colors, exit any other color-intensive applications in use.

Limit Netscape Colors

Step 1 Close the current session of Netscape.

Step 2 Launch Netscape from the command line by typing:

`netscape -install` (installs Netscape colors for Netscape use)

or

`netscape -ncols 32` (limits Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option)

1.7.2 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, you are unable to launch CTC Help and receive an "MSIE is not the default browser" error message.

Possible Cause Loss of association between browser and Help files.

Recommended Action When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as the default browser so that CTC associates the Help files to the correct browser. Complete the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-46 to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

Step 1 Open the Internet Explorer browser.

Step 2 From the menu bar, click **Tools > Internet Options**. The Internet Options window appears.

Step 3 In the Internet Options window, click the **Programs** tab.

Step 4 Click the **Internet Explorer should check to see whether it is the default browser** check box.

Step 5 Click **OK**.

Step 6 Exit any and all open and running CTC and Internet Explorer applications.

Step 7 Launch Internet Explorer and open a new CTC session. You should now be able to access the CTC Help.

1.7.3 Unable to Change Node View to Network View

Symptom When activating a large, multinode BLSR from Software R3.2 to Software R3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

Possible Cause The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.

Recommended Action Reset the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-46 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-47 to enable the CTC_HEAP variable change.

Note This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

Reset the CTC_HEAP Environment Variable for Windows

Step 1 Exit any and all open and running CTC and Netscape applications.

Step 2 From the Windows Desktop, right-click My Computer and choose **Properties** in the shortcut menu.

Step 3 In the System Properties window, click the **Advanced** tab.

Step 4 Click **Environment Variables** to open the Environment Variables window.

Step 5 Click **New** under the User variables field or the System variables field.

Step 6 Type **CTC_HEAP** in the Variable Name field.

Step 7 Type **256** in the Variable Value field, and then click **OK** to create the variable.

Step 8 Click **OK** in the Environment Variables window to accept the changes.

Step 9 Click **OK** in the System Properties window to accept the changes.

Restart the browser and CTC software.

Reset the CTC_HEAP Environment Variable for Solaris

Step 1 From the user shell window, kill any CTC applications.

Step 2 Kill any Netscape applications.

Step 3 In the user shell window, set the environment variable to increase the heap size:

```
% setenv CTC_HEAP 256
```

Step 4 Restart the browser and CTC software in the same user shell window.

1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2

Symptom The browser stalls or hangs when downloading a CTC JAR file from the TCC2 card.

Possible Cause McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.

Recommended Action Disable the VirusScan Download Scan feature. Complete the "Disable the VirusScan Download Scan" procedure on page 1-47.

Disable the VirusScan Download Scan

Step 1 From the Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.

Step 2 Double-click the **VShield** icon listed in the VirusScan Console dialog box.

Step 3 Click **Configure** on the lower part of the Task Properties window.

Step 4 Click the **Download Scan** icon on the left of the System Scan Properties dialog box.

Step 5 Uncheck the **Enable Internet download scanning** check box.

Step 6 Click **Yes** when the warning message appears.

Step 7 Click **OK** in the System Scan Properties dialog box.

Step 8 Click **OK** in the Task Properties window.

Step 9 Close the McAfee VirusScan window.

1.7.5 CTC Does Not Launch

Symptom CTC does not launch; usually an error message appears before the login window appears.

Possible Cause The Netscape browser cache might point to an invalid directory.

Recommended Action Redirect the Netscape cache to a valid directory. Complete the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-48.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 open the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

Step 5 Change your disk cache folder to point to the cache file location.

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

1.7.6 Slow CTC Operation or Login Problems

Symptom You experience slow CTC operation or have problems logging into CTC.

Possible Cause The CTC cache file might be corrupted or might need to be replaced.

Recommended Action Delete the CTC cache file. This operation forces the ONS 15454 to download a new set of JAR files to your computer hard drive. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-48 or the "Delete the CTC Cache File Manually" procedure on page 1-49.

Delete the CTC Cache File Automatically

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting CTC cache might cause any CTC running on this system to behave in an unexpected manner.

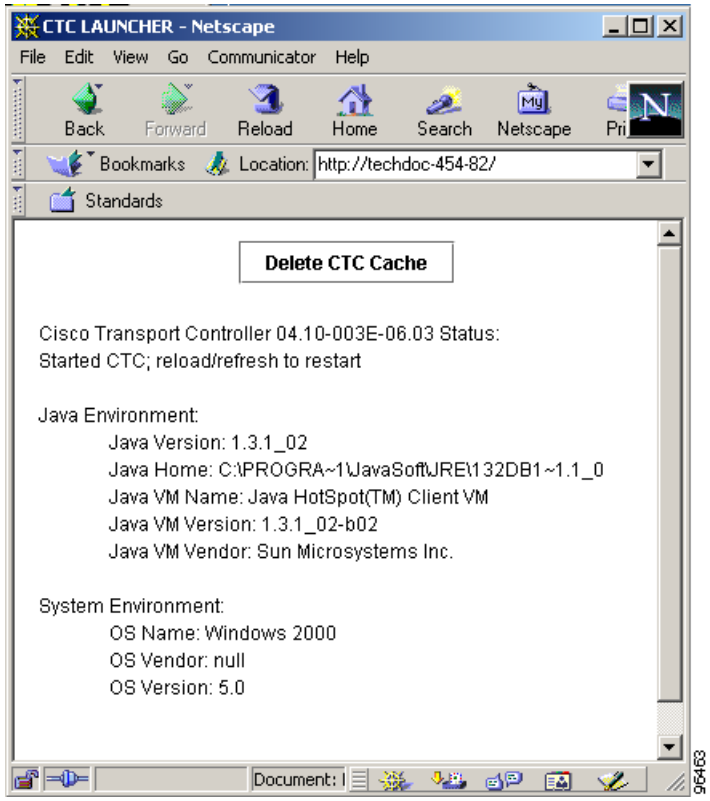
Step 1 Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2 Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.

Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-21 shows the Delete CTC Cache window.

Note For CTC releases earlier than R3.0, automatic deletion is unavailable. For CTC cache file manual deletion, complete the "Delete the CTC Cache File Manually" procedure on page 1-49.

Figure 1-21 Deleting the CTC Cache



Delete the CTC Cache File Manually

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

Step 1 To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.

Step 2 Enter *.jar in the Search for files or folders named field in the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2. These files might include CTC*.jar, CMS*.jar, and jar_cache*.tmp.

Step 4 Highlight the files and press the keyboard **Delete** key.

Step 5 Click **Yes** in the Confirm dialog box.

1.7.7 Node Icon is Gray on CTC Network View

Symptom The CTC network view shows one or more node icons as gray in color and without a node name.

Possible Cause Different CTC releases not recognizing each other.

Recommended Action Correct the core version build as described in the "Different CTC Releases Do Not Recognize Each Other" section on page 1-52.

Possible Cause A username/password mismatch.

Recommended Action Correct the username and password as described in the "Username or Password Do Not Match" section on page 1-53.

Possible Cause No IP connectivity between nodes.

Recommended Action Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "Ethernet Connections" section on page 1-55.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.7.8 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.

Possible Cause You are logging into a node running CTC Software R4.0 or earlier. Releases earlier than R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.

Recommended Action Install the software CD for the release of the node you are logging into. Run the CTC Setup Wizard (double-click **Setup.exe**). Choose **Custom installation**, then choose the Java Policy option. For additional information, refer to the CTC installation information in the *Cisco ONS 15454 Procedure Guide*. If the software CD is not available, you must manually edit the java.policy file on your computer. Complete the "Manually Edit the java.policy File" procedure on page 1-50.

Manually Edit the java.policy File

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

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

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

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

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

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as **.java.policy**. On Win98/2000 PCs, save the file to the C:\Windows folder. On Windows NT 4.0 or later PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.7.9 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Possible Cause The compatible Java 2 JRE is not installed.

Recommended Action The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-52. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-3 shows JRE compatibility with ONS 15454 software releases.

Table 1-3 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R2.2.1 and earlier	Yes	No	No
ONS 15454 R2.2.2	Yes	Yes	No
ONS 15454 R3.0	Yes	Yes	No
ONS 15454 R3.1	Yes	Yes	No
ONS 15454 R3.2	Yes	Yes	No
ONS 15454 R3.3	Yes	Yes	No
ONS 15454 R3.4	No	Yes	No
ONS 15454 R4.0[1]	No	Yes	No
ONS 15454 R4.1	No	Yes	No
ONS 15454 R4.5	No	Yes	No

Table 1-3 JRE Compatibility (continued)

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R4.6	No	Yes	Yes
ONS 15454 R4.7	No	No	Yes

1. Software R4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

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

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

Note After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the core and element builds discovered on the network.

1.7.10 Different CTC Releases Do Not Recognize Each Other

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

Possible Cause The software loaded on the connecting workstation and the software on the TCC2 card are incompatible.

Recommended Action This occurs when the TCC2 software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-52.

Note Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node.

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

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

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

Note After R2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 R1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the core and element builds discovered on the network.

1.7.11 Username or Password Do Not Match

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

Possible Cause The username or password entered does not match the information stored in the TCC2.

Recommended Action All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, type the CISCO15 user name in capital letters and click **Login** (no password is required). If you are using a CTC Software R2.2.2 or earlier and CISCO15 does not work, type cerent454 for the user name. Complete the "Verify Correct Username and Password" procedure on page 1-53.

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 Technical Support (1 800 553-2447) to have them enter your system and create a new user name and password.

1.7.12 No IP Connectivity Exists Between Nodes

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

Possible Cause A lost Ethernet connection.

Recommended Action Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "Ethernet Connections" section on page 1-55.

1.7.13 DCC Connection Lost

Symptom The node is usually accompanied by alarms and the nodes in the network view have a gray icon. This symptom is usually accompanied by an EOC alarm.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.7.14 "Path in Use" Error When Creating a Circuit

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

Possible Cause Another user has already selected the same source port to create another circuit.

Recommended Action CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. Cancel the circuit creation and start over, or click **Back** until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.

1.7.15 Calculate and Design IP Subnets

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

Possible Cause The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.

Recommended Action Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 IP capability, refer to the *Cisco ONS 15454 Reference Manual.*

1.7.16 Ethernet Connections

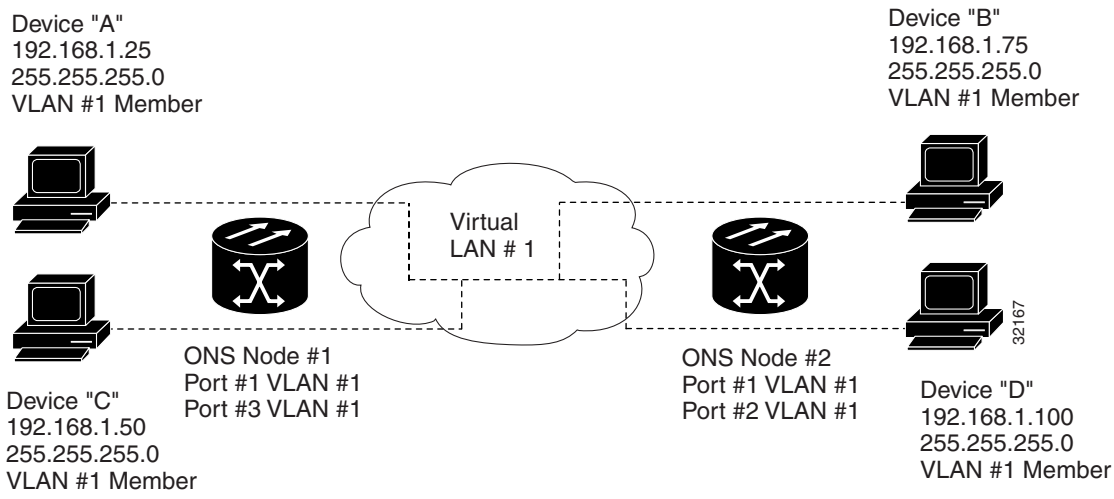
Symptom Ethernet connections appear to be broken or are not working properly.

Possible Cause Improperly seated connections.

Possible Cause Incorrect connections.

Recommended Action You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-22 when using the steps in the "Verify Ethernet Connections" procedure on page 1-55.

Figure 1-22 Ethernet Connectivity Reference



Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET and dense wavelength division multiplexing (DWDM) alarms on the STS that carries the VLAN Ethernet circuit. Clear any alarms by looking them up in Chapter 2, "Alarm Troubleshooting."

Step 3 Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 2, "Alarm Troubleshooting."

Step 4 Verify that the ACT LED on the Ethernet card is green.

Step 5 Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.

Step 6 If no green link-integrity LED is illuminated for any of these ports:

- **a.** Verify physical connectivity between the ONS 15454s and the attached device.
- **b.** Verify that the ports are enabled on the Ethernet cards.
- **c.** Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

d. Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.

e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the "Verify General Card LED Operation" procedure on page 1-28.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices. Complete the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-43. If the ping is unsuccessful:

a. Verify that device A and device C are on the same IP subnet.

b. open the Ethernet card in CTC card view and click the **Provisioning > VLAN** tab to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.

c. If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.

Step 8 Repeat Step 7 for devices B and D.

Step 9 Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

1.7.17 VLAN Cannot Connect to Network Device from Untag Port

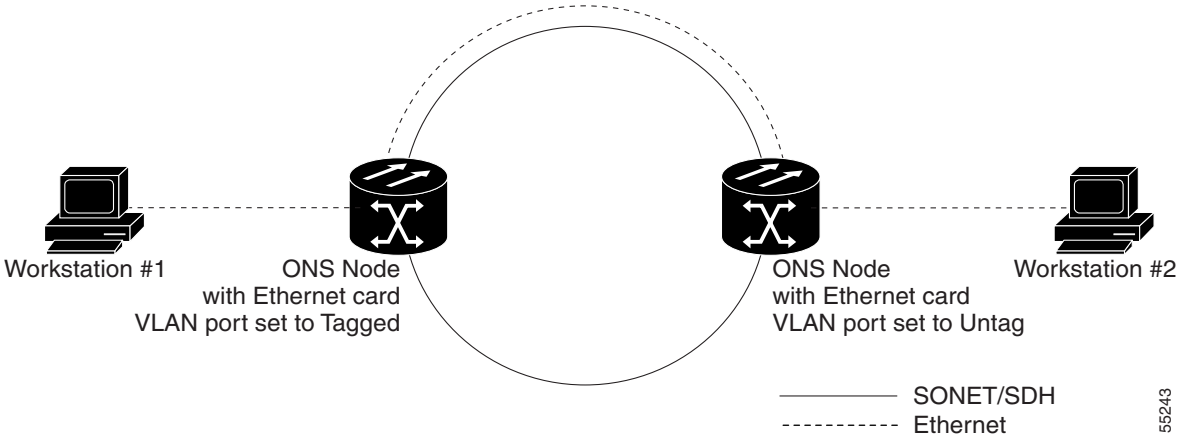
Symptom Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-23). They might also see a higher than normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Possible Cause The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.

Possible Cause 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.

Recommended Action The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non-IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance.

Figure 1-23 VLAN with Ethernet Ports at Tagged and Untag

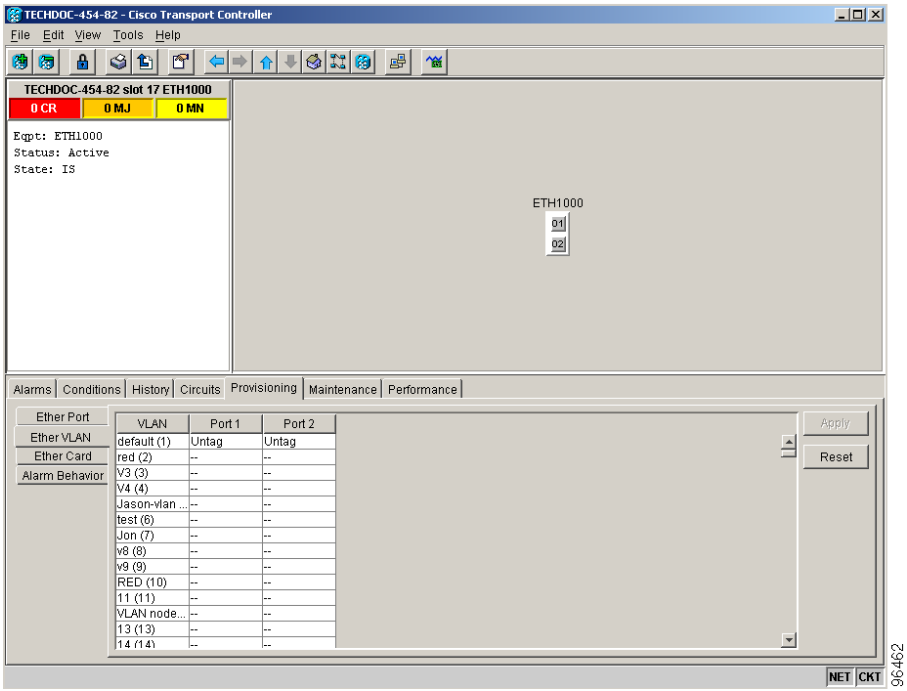


Change VLAN Port Tag and Untagged Settings

Step 1 Display the CTC card view for the Ethernet card involved in the problem VLAN.

Step 2 Click the **Provisioning > Ether VLAN** tab (Figure 1-24).

Figure 1-24 Configuring VLAN Membership for Individual Ethernet Ports



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

Step 4 At the VLAN port set to **Untag**, click the port and choose **Tagged**.

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

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

1.8 Circuits and Timing

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

1.8.1 OC-N Circuit Transitions to Partial State

Symptom An automatic or manual transition of a circuit from one state to another state results in the OOS-PARTIAL status, which indicates that not all OC-N connections in the circuit are in the IS-NR service state.

Possible Cause During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.

Recommended Action Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-58. Log into the circuit node that did not change to the desired state and determine the version of software. If the software on the node is Software R3.3 or earlier, upgrade the software. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures.

Note If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by using only the circuit state supported in the earlier software version.

Possible Cause During an automatic transition, some path-level defects and/or alarms were detected on the circuit.

Possible Cause One end of the circuit is not properly terminated.

Recommended Action Determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-58. Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of OC-N Circuit Nodes

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the *_PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab (if you are viewing a SONET circuit).

The State tab window lists the Node, End A, End B, CRS admin state, and CRS Service State for each of the nodes in the circuit.

1.8.2 AIS-V on DS3XM-6 Unused VT Circuits

Symptom An incomplete circuit path causes an AIS.

Possible Cause 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.

Recommended Action An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth. Complete the "Clear AIS-V on DS3XM-6 or DS3XM12 Unused VT Circuits" procedure on page 1-59.

Clear AIS-V on DS3XM-6 or DS3XM12 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** check box in the circuit creation window.

Step 5 Give the unidirectional VT circuit an easily recognizable name, such as "`delete me`."

Step 6 Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** tab.

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**. Do not check any check boxes.

Step 11 Click **Yes** in the Delete Confirmation dialog box.

Step 12 Display the DS3XM-6 or DS3XM12 card in CTC card view. Click **Maintenance > DS1**.

Step 13 Locate the VT in Facility (line) Loopback.

Step 14 From the Loopback Type list, choose **None** and then click **Apply**.

Step 15 Click the **Alarms** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the DS3XM-6 or DS3XM12 cards.

1.8.3 Circuit Creation Error with VT1.5 Circuit

Symptom You receive an "Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at *node_name*" message when trying to create a VT1.5 circuit in CTC.

Possible Cause You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message.

Recommended Action The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a path protection or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

1.8.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 or DS3XM12 Card

Symptom You cannot create a circuit from a DS-3 card to a DS3XM-6 or DS3XM12 card.

Possible Cause A DS-3 card and a DS3XM-6 or DS3XM12 card have different functions.

Recommended Action A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. The DS3XM12 converts each of its 12 interfaces into up to 48 DS-1s. Thus, you can create a circuit from a DS3XM-6 or DS3XM12 card to a DS-1 card, but not from a DS3XM 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 or DS3XM12 has a VT payload with a C2 hex value of 02.

Note You can find instructions for creating circuits in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

1.8.5 DS-3 Card Does Not Report AIS-P From External Equipment

Symptom A DS3-12, DS3N-12, DS3-12E, or DS3N-12E card does not report STS AIS-P from the external equipment/line side.

Possible Cause The card is functioning as designed.

Recommended Action This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. DS3-12, DS3N-12, DS3-12E, and DS3N-12E cards have DS3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information about the PM capabilities of the DS3-12, DS3N-12, DS3-12E or DS3N-12E cards, refer to the *Cisco ONS 15454 Reference Manual*.

1.8.6 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Possible Cause OC-3 and DCC have limitations for the ONS 15454.

Recommended Action For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Procedure Guide*.

1.8.7 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Possible Cause The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.

Possible Cause The optical or building integrated timing supply (BITS) input is not functioning.

Possible Cause The synchronization status messaging (SSM) message is set to do not use for synchronization (DUS).

Possible Cause SSM indicates a Stratum 3 or lower clock quality.

Possible Cause The input frequency is off by more than 15 ppm.

Possible Cause The input clock wanders and has more than three slips in 30 seconds.

Possible Cause A bad timing reference existed for at least two minutes.

Recommended Action The ONS 15454 internal clock operates at a Stratum 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of ± 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x 10^{-7}/day, including temperature. ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.

1.8.8 Holdover Synchronization Alarm

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

Possible Cause The last reference input has failed.

Recommended Action The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the "HLDOVRSYNC" section on page 2-116 for a detailed description of this alarm.

Note The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

1.8.9 Free-Running Synchronization Mode

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

Possible Cause No reliable reference input is available.

Recommended Action The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" condition on page 2-103 for a detailed description.

1.8.10 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy chain the BITS sources.

Possible Cause Daisy-chained BITS sources are not supported on the ONS 15454.

Recommended Action Daisy-chained BITS sources cause additional wander buildup in the network and are therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

1.8.11 Blinking STAT LED after Installing a Card

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

Possible Cause The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.

Recommended Action The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an "EQPT" alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Air Filter and Fan Procedures" procedure on page 2-257.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

1.9 Fiber and Cabling

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

1.9.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Possible Cause Faulty cabling or low optical-line levels.

Recommended Action 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 "Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2. Troubleshoot low optical levels using the "Faulty Fiber-Optic Connections" section on page 1-63.

1.9.2 Faulty Fiber-Optic Connections

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

Possible Cause Faulty fiber-optic connections.

Recommended Action Faulty fiber-optic connections can be the source of SONET/DWDM alarms and signal errors. Complete the "Verify Fiber-Optic Connections" procedure on page 1-64.

Possible Cause Faulty CAT-5 cables.

Recommended Action Faulty CAT-5 cables can be the source of SONET/DWDM alarms and signal errors. Complete the "Crimp Replacement LAN Cables" section on page 1-65.

Possible Cause Faulty Gigabit Interface Converters (GBIC).

Recommended Action Faulty GBICs can be the source of SONET/DWDM alarms and signal errors. See the "Replace Faulty GBIC or SFP Connectors" section on page 1-67.

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

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.

Note SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

- **a.** Remove the Rx end of the suspect fiber.
- **b.** Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.
- **c.** Determine the power level of fiber with the fiber-optic power meter.
- **d.** Verify the power meter is set to the appropriate wavelength for the OC-N card being tested (either 1310 nm or 1550 nm depending on the specific card).
- **e.** Verify that the power level falls within the range specified for the card if it is an OC-N card; see the "OC-N Card Transmit and Receive Levels" section on page 1-71.

Step 4 If the power level falls below the specified range for the OC-N card:

- **a.** Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- **b.** Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- **c.** Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.

  IR cards transmit a lower output power than LR cards.
- **d.** Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

- **e.** If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):
  - Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
  - Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
  - Excessive number of fiber splices; splices take approximately 0.5 dB each.

Note These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the OC-N card failed.

a. Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.

b. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the power level on the fiber is above the range specified for the card, ensure that an ONS LR card is not being used when an ONS IR card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter will be too powerful for the receiver on the receiving OC-N card.

Receiver overloads occur when maximum receiver power is exceeded.

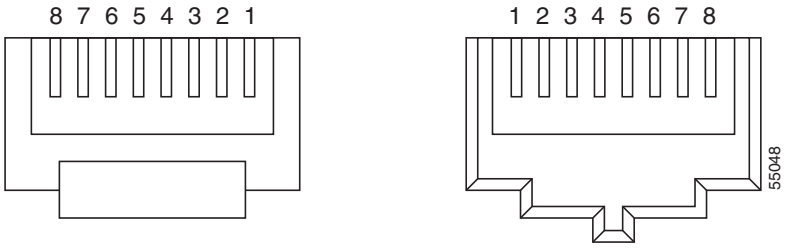
Tip To prevent overloading the receiver, use an attenuator on the fiber between the ONS OC-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS OC-N cards. Refer to the attenuator documentation for specific instructions.

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

1.9.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-25 shows the wiring of an RJ-45 connector. Figure 1-26 shows a LAN cable layout, and Table 1-4 shows the cable pinouts. Figure 1-27 shows a cross-over cable layout, and Table 1-5 shows the cross-over pinouts.

Figure 1-25 RJ-45 Pin Numbers



End view of RJ-45 plug — Looking into an RJ-45 jack

Figure 1-26 LAN Cable Layout

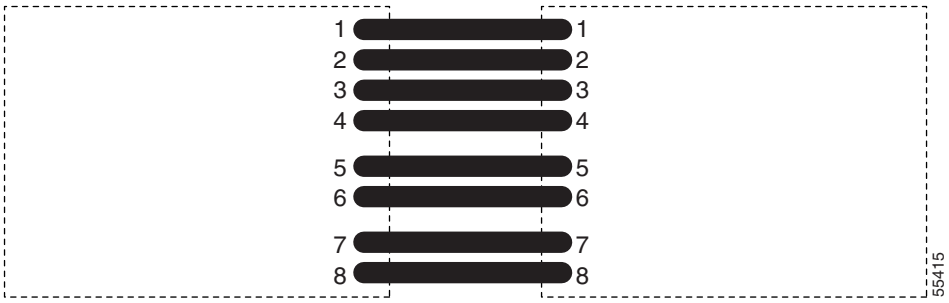


Table 1-4 LAN Cable Pinout

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

Figure 1-27 Cross-Over Cable Layout

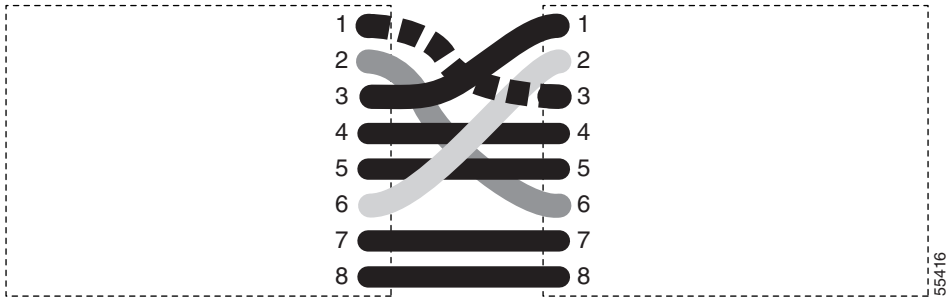


Table 1-5 Cross-Over Cable Pinout

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

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

1.9.2.2 Replace Faulty GBIC or SFP Connectors

GBICs and small form-factor pluggables (SFP) are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning **GBICs are Class I laser products. These products have been tested and comply with Class I limits.**

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

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities, see Table 1-6 and Table 1-7 on page 1-68, and refer to the *Cisco ONS 15454 Reference Manual*.

Note GBICs and SFPs must be matched on either end by type: SX to SX, LX to LX, or ZX to ZX.

Note DWDM and coarse wavelength division multiplexing (CWDM) GBICs do not function with Software R4.7.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G-Series, or G1K-4 card. The other model has a locking handle. Both models are shown in Figure 1-28.

Figure 1-28 GBICs

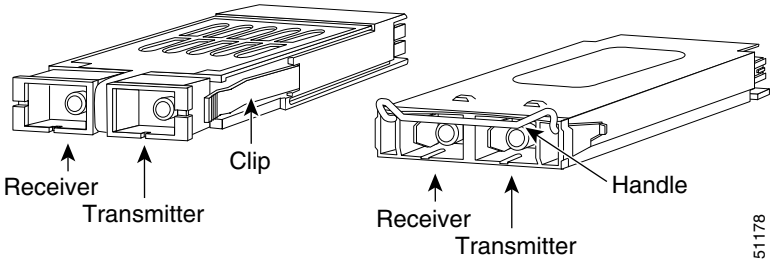


Table 1-6 shows the available GBICs. Table 1-7 shows the available SFPs.

Note GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Table 1-6 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G-Series G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=
1000BaseLX	E1000-2-G G-Series G1K-4	Long reach	Single-mode fiber up to 10 km long	15454E-GBIC-LX=
1000BaseZX	G-Series G1K-4	Extra long reach	Single-mode fiber up to 70 km long	15454E-GBIC-ZX=

Table 1-7 Available SFPs

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	ML1000-2	Short reach	Multimode fiber up to 550 m long	15454E-SFP-LC-SX=
1000BaseLX	ML1000-2	Long reach	Single-mode fiber up to 10 km long	15454E-SFP-LC-LX=

Remove GBIC or SFP Connectors

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector.

Warning **Invisible laser radiation might be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Step 2 Release the GBIC or SFP from the slot by simultaneously squeezing the two plastic tab on each side.

Step 3 Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Installing a GBIC with Clips

Step 1 Remove the GBIC from its protective packaging.

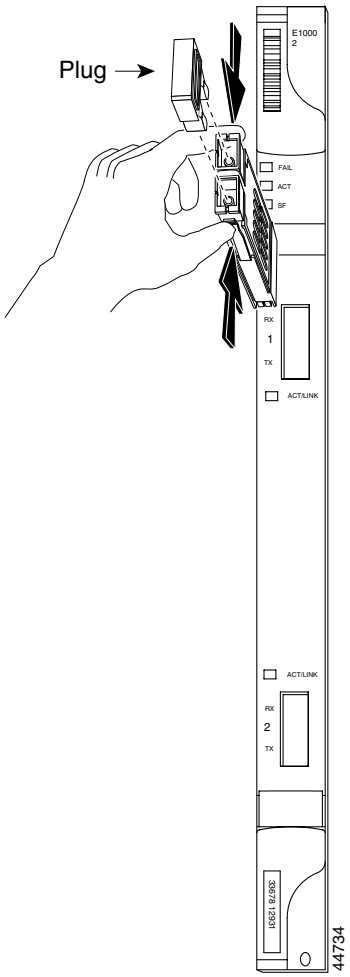
Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G-Series card (Figure 1-29).

Note GBICs are keyed to prevent incorrect installation.

Figure 1-29 GBIC Installation (with Clips)



Step 5 Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

Step 7 Return to your originating procedure (NTP).

Installing a GBIC with a Handle

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Remove the protective plug from the SC-type connector.

Step 5 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, G1K-4, or G-Series card.

Note GBICs are keyed to prevent incorrect installation.

Step 6 Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.

Step 7 Return to your originating procedure (NTP).

1.9.3 OC-N Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate. Table 1-8 lists these levels.

Table 1-8 OC-N Card Transmit and Receive Levels

OC-N Card	Receive	Transmit
OC3 IR4/STM1SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC3 IR/STM 1SH 1310-8	–30 to –8 dBm	–15 to –8 dBm
OC12 IR/STM4 SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC12 LR/STM4 LH 1310	–28 to –8 dBm	–3 to +2 dBm
OC12 LR/STM4 LH 1550	–28 to –8 dBm	–3 to +2 dBm
OC12 IR/STM4 SH 1310-4	–28 to –8 dBm	–3 to +2 dBm
OC48 IR/STM16 SH AS 1310	–18 to 0 dBm	–5 to 0 dBm
OC48 LR/STM16 LH AS 1550	–28 to –8 dBm	–2 to +3 dBm
OC48 ELR/STM16 EH 100GHz	–28 to –8 dBm	–2 to 0 dBm
OC192 SR/STM64 IO 1310	–11 to –1 dBm	–6 to –1 dBm
OC192 IR STM64 SH 1550	–14 to –1 dBm	–1 to +2 dBm
OC192 LR/STM64 LH 1550	–21 to –9 dBm	+7 to +10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	–22 to –9 dBm	+3 to +6 dBm
TXP-MR-10G Trunk side: Client side:	 –26 to –8 dBm –14 to –1 dBm	 –16 to +3 dBm –6 to –1 dBm
MXP-2.5G-10G Trunk side: Client side:	 –26 to –8 dBm depends on SFP	 –16 to +3 dBm depends on SFP

1.10 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.

Possible Cause Loss of power or low voltage.

Possible Cause Improperly connected power supply.

Recommended Action The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tab and change the Date and Time fields. Complete the "Isolate the Cause of Power Supply Problems" procedure on page 1-72.

Warning **When working with live power, always use proper tools and eye protection.**

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

Caution Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15454 show signs of fluctuating power or power loss:

a. Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.

b. Verify that the power cable is #12 or #14 AWG and in good condition.

c. Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.

d. Verify that 20-A fuses are used in the fuse panel.

e. Verify that the fuses are not blown.

f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.

g. Verify that the DC power source has enough capacity to carry the power load.

h. If the DC power source is battery-based:

- Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.
- Check the age of the batteries. Battery performance decreases with age.
- Check for opens and shorts in batteries, which might affect power output.
- If brownouts occur, the power load and fuses might be too high for the battery plant.

Step 2 If multiple pieces of site equipment show signs of fluctuating power or power loss:

a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.

b. Check for excessive power drains caused by other equipment, such as generators.

c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

1.10.1 Power Consumption for Node and Cards

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

Possible Cause Improper power supply.

Recommended Action Refer to power information in the *Cisco ONS 15454 Reference Guide*.

Alarm Troubleshooting

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

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-6 provides a list of alarms organized alphabetically. Table 2-8 gives definitions of all ONS 15454 alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-12.

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call the Cisco Technical Assistance Center (Cisco TAC) to report a service-affecting problem (1 800 553-2447).

More information about alarm profile information modification and downloads are located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note Release 4.7 is DWDM only. It supports all DWDM, transponder (TXP), and muxponder (MXP) cards but not optical, electrical, fibre storage, or Ethernet cards.

2.1 Alarm Index by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15454 system. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.

Note The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15454 Critical alarms.

Table 2-1 ONS 15454 Critical Alarm Index

AS-MT-OOG, page 2-36 for an STS	IMPROPRMVL, page 2-118	MEA (BIC), page 2-167
AUTOLSROFF, page 2-38	LOA, page 2-130	MEA (EQPT), page 2-168
AWG-FAIL, page 2-43	LOF (DS3), page 2-133	MEA (PPM), page 2-171
AWG-OVERTEMP, page 2-43	LOF (EC1-12), page 2-134	MFGMEM, page 2-172
BKUPMEMP, page 2-45	LOF (OCN), page 2-134	OPWR-HFAIL, page 2-182
CKTDOWN, page 2-55	LOF (TRUNK), page 2-135	OPWR-LFAIL, page 2-183
COMIOXC, page 2-58	LOM, page 2-136	OTUK-LOF, page 2-185
CTNEQPT-PBPROT, page 2-63	LOP-P, page 2-136	PLM-P, page 2-190
CTNEQPT-PBWORK, page 2-65	LOS (2R), page 2-139	PORT-MISMATCH, page 2-193
EQPT, page 2-75	LOS (DS3), page 2-141	SQM, page 2-215 for STSTRM
EQPT-MISS, page 2-76	LOS (EC1-12), page 2-141	SWMTXMOD, page 2-219
FAN, page 2-89	LOS (OCN), page 2-144	TIM, page 2-225 (for TRUNK)
GAIN-HFAIL, page 2-106	LOS (OTS), page 2-146	TIM-P, page 2-226 (for STSTRM)
GAIN-LFAIL, page 2-107	LOS (TRUNK), page 2-147	UNEQ-P, page 2-231
GE-OOSYNC, page 2-107	LOS-P (OCH, OMS, OTS), page 2-150	VOA-HFAIL, page 2-236
HITEMP, page 2-115 (for NE)	LOS-P (TRUNK), page 2-151	VOA-LFAIL, page 2-237
I-HITEMP, page 2-117	MEA (AIP), page 2-166	—

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15454 Major alarms.

Table 2-2 ONS 15454 Major Alarm Index

APC-DISABLED, page 2-27	EOC, page 2-72	LOS (ISC), page 2-144
APSCM, page 2-31	EOC-L, page 2-74	LWBATVG, page 2-164
APSCNMIS, page 2-32	E-W-MISMATCH, page 2-79	MEM-GONE, page 2-172
AS-MT-OOG, page 2-36 for VT	EXTRA-TRAF-PREEMPT, page 2-83	OPTNTWMIS, page 2-179
AU-LOF, page 2-38	FC-NO-CREDITS, page 2-89	PEER-NORESPONSE, page 2-189
BAT-FAIL, page 2-44	FEC-MISM, page 2-91	PTIM, page 2-194
BLSROSYNC, page 2-45	GCC-EOC, page 2-107	PLM-V, page 2-191
BPV, page 2-46	GFP-CSF, page 2-108	PRC-DUPID, page 2-193
CARLOSS (E100T, E1000F), page 2-46	GFP-DE-MISMATCH, page 2-108	RCVR-MISS, page 2-198
CARLOSS (EQPT), page 2-48	GFP-EX-MISMATCH, page 2-109	RING-ID-MIS, page 2-201

Table 2-2 ONS 15454 Major Alarm Index (continued)

CARLOSS (G1000), page 2-49	GFP-LFD, page 2-110	RING-MISMATCH, page 2-201
CARLOSS (GE), page 2-52	GFP-NO-BUFFERS, page 2-110	SIGLOSS, page 2-211
CARLOSS (ISC), page 2-52	GFP-UP-MISMATCH, page 2-111	SQM, page 2-215 (VT-TERM)
CARLOSS (ML100T, ML1000, ML2), page 2-53	HIBATVG, page 2-112	SSM-FAIL, page 2-215 for double failure
CARLOSS (TRUNK), page 2-54	HLDOVRSYNC, page 2-116	SYNCLOSS, page 2-222
CONTBUS-A-18, page 2-59	INVMACADR, page 2-121	SYSBOOT, page 2-225
CONTBUS-B-18, page 2-60	LASERBIAS-DEG, page 2-125	TPTFAIL (FCMR), page 2-227
CONTBUS-IO-A, page 2-60	LASERBIAS-FAIL, page 2-125	TPTFAIL (G1000), page 2-227
CONTBUS-IO-B, page 2-61	LASEREOL, page 2-126	TPTFAIL (ML1000, ML100T, ML2), page 2-228
DBOSYNC, page 2-66	LASERTEMP-DEG, page 2-126	TRMT, page 2-229
DSP-COMM-FAIL, page 2-68	LOF (BITS), page 2-131	TRMT-MISS, page 2-230
DSP-FAIL, page 2-68	LOF (DS1), page 2-132	UNEQ-V, page 2-233
DUP-IPADDR, page 2-68	LOP-V, page 2-137	UT-COMM-FAIL, page 2-234
DUP-NODENAME, page 2-69	LOS (BITS), page 2-139	UT-FAIL, page 2-235
EHIBATVG, page 2-69	LOS (DS1), page 2-140	WVL-MISMATCH, page 2-238
ELWBATVG, page 2-70	—	—

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15454 Minor alarms.

Table 2-3 ONS 15454 Minor Alarm Index

APSB, page 2-28	HELLO, page 2-111	PORT-ADD-PWR-FAIL-HI, page 2-191
APSCDFLTK, page 2-29	HI-LASERBIAS, page 2-112	PORT-ADD-PWR-FAIL-LOW, page 2-192
APSC-IMP, page 2-29	HI-LASERTEMP, page 2-113	PROTNA, page 2-194
APSCINCON, page 2-30	HI-RXPOWER, page 2-114	PWR-FAIL-A, page 2-195
APS-INV-PRIM, page 2-33	HITEMP, page 2-115 (EQPT)	PWR-FAIL-B, page 2-196
APSMM, page 2-34	HI-TXPOWER, page 2-116	PWR-FAIL-RET-A, page 2-196
APS-PRIM-SEC-MISM, page 2-34	KBYTE-APS-CHANNEL-FAILURE, page 2-124	PWR-FAIL-RET-B, page 2-197
AUTORESET, page 2-39	LASEREOL, page 2-126	RSVP-HELLODOWN, page 2-202
AUTOSW-LOP (VT-MON), page 2-41	LMP-HELLODOWN, page 2-130	SFTWDOWN, page 2-209
AUTOSW-UNEQ (VT-MON), page 2-42	LMP-NDFAIL, page 2-130	SH-INS-LOSS-VAR-DEG-HIGH, page 2-210
AWG-DEG, page 2-43	LO-LASERTEMP, page 2-135	SH-INS-LOSS-VAR-DEG-LOW, page 2-210

Table 2-3 ONS 15454 Minor Alarm Index (continued)

CASETEMP-DEG, page 2-54	LO-RXPOWER, page 2-138	SNTP-HOST, page 2-211
COMM-FAIL, page 2-58	LOS (FUDC), page 2-143	SSM-FAIL, page 2-215
DATAFLT, page 2-66	LOS (MSUDC), page 2-144	SYNCPRI, page 2-223
ERROR-CONFIG, page 2-77	LOS-O, page 2-148	SYNCSEC, page 2-223
EXCCOL, page 2-81	LO-TXPOWER, page 2-152	SYNCTHIRD, page 2-224
EXT, page 2-82	MEM-LOW, page 2-172	TIM-MON, page 2-226
FEPRLF, page 2-100	OPWR-HDEG, page 2-180	TIM-P, page 2-226 (STSMON)
FIBERTEMP-DEG, page 2-101	OPWR-LDEG, page 2-182	UNREACHABLE-TARGET-POWER, page 2-234
FSTSYNC, page 2-104	PORT-ADD-PWR-DEG-HI, page 2-191	VOA-HDEG, page 2-236
GAIN-HDEG, page 2-105	PORT-ADD-PWR-DEG-LOW, page 2-191	VOA-LDEG, page 2-237
GAIN-LDEG, page 2-106	—	—

2.1.4 NA Conditions

Table 2-4 alphabetically lists ONS 15454 Not Alarmed conditions.

Table 2-4 ONS 15454 NA Conditions Index

ALS, page 2-26	INC-ISD, page 2-119	OOU-TPT, page 2-179
AMPLI-INIT, page 2-26	INHSWPR, page 2-120	OSRION, page 2-183
APC-CORRECTION-SKIPPED, page 2-26	INHSWWKG, page 2-120	OTUK-SD, page 2-185
APC-END, page 2-27	INTRUSION-PSWD, page 2-121	OTUK-SF, page 2-186
APC-OUT-OF-RANGE, page 2-27	IOSCFGCOPY, page 2-123	OTUK-TIM, page 2-186
APSIMP, page 2-32	KB-PASSTHR, page 2-123	OUT-OF-SYNC, page 2-187
APS-PRIM-FAC, page 2-33	LAN-POL-REV, page 2-124	PARAM-MISM, page 2-187
AS-CMD, page 2-35	LASER-APR, page 2-125	PDI-P, page 2-188
AS-MT, page 2-36	LCAS-CRC, page 2-127	PORT-MISMATCH, page 2-193 for FCMR
AUD-LOG-LOSS, page 2-37	LCAS-RX-FAIL, page 2-128	RAI, page 2-197
AUD-LOG-LOW, page 2-37	LCAS-TX-ADD, page 2-128	RING-SW-EAST, page 2-202
AUTOSW-LOP (STSMON), page 2-40	LCAS-TX-DNU, page 2-129	RING-SW-WEST, page 2-202
AUTOSW-PDI, page 2-41	LKOUTPR-S, page 2-129	RUNCFG-SAVENEED, page 2-203
AUTOSW-SDBER, page 2-41	LOCKOUT-REQ, page 2-131	SD (TRUNK), page 2-203
AUTOSW-SFBER, page 2-42	LPBKCRS, page 2-153	SD (DS1, DS3), page 2-203
AUTOSW-UNEQ (STSMON), page 2-42	LPBKDS1FEAC, page 2-153	SD-L, page 2-205
AWG-WARM-UP, page 2-44	LPBKDS1FEAC-CMD, page 2-154	SD-P, page 2-206

Table 2-4 ONS 15454 NA Conditions Index (continued)

CLDRESTART, page 2-57	LPBKDS3FEAC, page 2-154	SD-V, page 2-206
CTNEQPT-MISMATCH, page 2-62	LPBKDS3FEAC-CMD, page 2-155	SF (TRUNK), page 2-207
DS3-MISM, page 2-67	LPBKFACILITY (TRUNK), page 2-155	SF (DS1, DS3), page 2-207
ETH-LINKLOSS, page 2-78	LPBKFACILITY(DS1, DS3), page 2-155	SF-L, page 2-208
EXERCISE-RING-FAIL, page 2-81	LPBKFACILITY (EC1-12), page 2-156	SF-P, page 2-209
EXERCISE-SPAN-FAIL, page 2-82	LPBKFACILITY (ESCON), page 2-156	SF-V, page 2-209
FAILTOSW, page 2-83	LPBKFACILITY (FC), page 2-157	SHUTTER-OPEN, page 2-210
FAILTOSW-PATH, page 2-84	LPBKFACILITY (FCMR), page 2-157	SPAN-SW-EAST, page 2-212
FAILTOSWR, page 2-85	LPBKFACILITY (G1000), page 2-157	SPAN-SW-WEST, page 2-212
FAILTOSWS, page 2-87	LPBKFACILITY (GE), page 2-158	SQUELCH, page 2-212
FE-AIS, page 2-90	LPBKFACILITY (ISC), page 2-158	SQUELCHED, page 2-214
FE-DS1-MULTLOS, page 2-91	LPBKFACILITY (ML2), page 2-159	SSM-DUS, page 2-215
FE-DS1-NSA, page 2-92	LPBKFACILITY (OCN), page 2-159	SSM-LNC, page 2-216
FE-DS1-SA, page 2-92	LPBKTERMINAL (TRUNK), page 2-159	SSM-OFF, page 2-216
FE-DS1-SNGLLOS, page 2-93	LPBKTERMINAL (DS1, DS3), page 2-160	SSM-PRC, page 2-216
FE-DS3-NSA, page 2-93	LPBKTERMINAL (EC1-12), page 2-160	SSM-PRS, page 2-217
FE-DS3-SA, page 2-94	LPBKTERMINAL (ESCON), page 2-161	SSM-RES, page 2-217
FE-EQPT-NSA, page 2-94	LPBKTERMINAL (FC), page 2-161	SSM-SDN-TN, page 2-217
FE-FRCDWKSWBK-SPAN, page 2-95	LPBKTERMINAL (FCMR), page 2-161	SSM-SETS, page 2-217
FE-FRCDWKSWPR-RING, page 2-96	LPBKTERMINAL (G1000), page 2-162	SSM-SMC, page 2-217
FE-FRCDWKSWPR-SPAN, page 2-96	LPBKTERMINAL (GE), page 2-162	SSM-ST2, page 2-218
FE-IDLE, page 2-97	LPBKTERMINAL (ISC), page 2-163	SSM-ST3, page 2-218
FE-LOCKOUTOFPR-SPAN, page 2-97	LPBKTERMINAL (ML2), page 2-163	SSM-ST3E, page 2-218
FE-LOF, page 2-98	LPBKTERMINAL (OCN), page 2-163	SSM-ST4, page 2-218
FE-LOS, page 2-98	MAN-REQ, page 2-164	SSM-STU, page 2-219
FE-MANWKSWBK-SPAN, page 2-99	MANRESET, page 2-164	SSM-TNC, page 2-219
FE-MANWKSWPR-RING, page 2-99	MANSWTOINT, page 2-165	SWTOPRI, page 2-221
FE-MANWKSWPR-SPAN, page 2-100	MANSWTOPRI, page 2-165	SWTOSEC, page 2-221
FORCED-REQ, page 2-101	MANSWTOSEC, page 2-165	SWTOTHIRD, page 2-221
FORCED-REQ-RING, page 2-102	MANSWTOTHIRD, page 2-165	SYNC-FREQ, page 2-222
FORCED-REQ-SPAN, page 2-102	MANUAL-REQ-RING, page 2-166	TIM, page 2-225 (for OCN only)
FRCDSWTOINT, page 2-102	MANUAL-REQ-SPAN, page 2-166	TX-RAI, page 2-230
FRCDSWTOPRI, page 2-103	NO-CONFIG, page 2-173	UNC-WORD, page 2-231
FRCDSWTOSEC, page 2-103	OCHNC-INC, page 2-174	VCG-DEG, page 2-235
FRCDSWTOTHIRD, page 2-103	ODUK-SD-PM, page 2-178	VCG-DOWN, page 2-235
FRNGSYNC, page 2-103	ODUK-SF-PM, page 2-178	WKSWPR, page 2-237

Table 2-4 ONS 15454 NA Conditions Index (continued)

FULLPASSTHR-BI, page 2-104	ODUK-TIM-PM, page 2-179	WTR, page 2-238
HI-CCVOLT, page 2-112	—	—

2.1.5 NR Conditions

Table 2-5 alphabetically lists ONS 15454 Not Reported conditions.

Table 2-5 ONS 15454 NR Conditions Index

AIS, page 2-24	ODUK-1-AIS-PM, page 2-174	OTUK-AIS, page 2-183
AIS-L, page 2-24	ODUK-2-AIS-PM, page 2-174	OTUK-BDI, page 2-184
AIS-P, page 2-25	ODUK-3-AIS-PM, page 2-175	RFI, page 2-198
AIS-V, page 2-25	ODUK-4-AIS-PM, page 2-175	RFI-L, page 2-199
AUTOSW-AIS, page 2-40	ODUK-AIS-PM, page 2-176	RFI-P, page 2-199
ERFI-P-CONN, page 2-76	ODUK-BDI-PM, page 2-176	RFI-V, page 2-200
ERFI-P-PAYLD, page 2-76	ODUK-LCK-PM, page 2-177	TX-AIS, page 2-230
ERFI-P-SRVR, page 2-77	ODUK-OCI-PM, page 2-177	—

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15454 alarms and conditions.

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index

AIS, page 2-24	FULLPASSTHR-BI, page 2-104	ODUK-AIS-PM, page 2-176
AIS-L, page 2-24	GAIN-HDEG, page 2-105	ODUK-BDI-PM, page 2-176
AIS-P, page 2-25	GAIN-HFAIL, page 2-106	ODUK-BDI-PM, page 2-176
AIS-V, page 2-25	GAIN-LDEG, page 2-106	ODUK-LCK-PM, page 2-177
ALS, page 2-26	GAIN-LFAIL, page 2-107	ODUK-OCI-PM, page 2-177
AMPLI-INIT, page 2-26	GCC-EOC, page 2-107	ODUK-SD-PM, page 2-178
APC-CORRECTION-SKIPPED, page 2-26	GE-OOSYNC, page 2-107	ODUK-SF-PM, page 2-178
APC-DISABLED, page 2-27	GFP-CSF, page 2-108	ODUK-TIM-PM, page 2-179
APC-END, page 2-27	GFP-DE-MISMATCH, page 2-108	OOU-TPT, page 2-179
APC-OUT-OF-RANGE, page 2-27	GFP-EX-MISMATCH, page 2-109	OPTNTWMIS, page 2-179
APSB, page 2-28	GFP-LFD, page 2-110	OPWR-HDEG, page 2-180
APSCDFLTK, page 2-29	GFP-NO-BUFFERS, page 2-110	OPWR-HFAIL, page 2-182
APSC-IMP, page 2-29	GFP-UP-MISMATCH, page 2-111	OPWR-LDEG, page 2-182
APSCINCON, page 2-30	HELLO, page 2-111	OPWR-LFAIL, page 2-183
APSCM, page 2-31	HIBATVG, page 2-112	OSRION, page 2-183

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

CARLOSS (ML100T, ML1000, ML2), page 2-53	LOF (EC1-12), page 2-134	RSVP-HELLODOWN, page 2-202
CARLOSS (TRUNK), page 2-54	LOF (OCN), page 2-134	RUNCFG-SAVENEED, page 2-203
CASETEMP-DEG, page 2-54	LOF (TRUNK), page 2-135	SD (TRUNK), page 2-203
CKTDOWN, page 2-55	LO-LASERTEMP, page 2-135	SD (DS1, DS3), page 2-203
CLDRESTART, page 2-57	LOM, page 2-136	SD-L, page 2-205
COMIOXC, page 2-58	LOP-P, page 2-136	SD-P, page 2-206
COMM-FAIL, page 2-58	LOP-V, page 2-137	SD-V, page 2-206
CONTBUS-A-18, page 2-59	LO-RXPOWER, page 2-138	SF (TRUNK), page 2-207
CONTBUS-B-18, page 2-60	LOS (2R), page 2-139	SF (DS1, DS3), page 2-207
CONTBUS-IO-A, page 2-60	LOS (BITS), page 2-139	SF-L, page 2-208
CONTBUS-IO-B, page 2-61	LOS (DS1), page 2-140	SF-P, page 2-209
CTNEQPT-MISMATCH, page 2-62	LOS (DS3), page 2-141	SF-V, page 2-209
CTNEQPT-PBPROT, page 2-63	LOS (EC1-12), page 2-141	SFTWDOWN, page 2-209
CTNEQPT-PBWORK, page 2-65	LOS (ESCON), page 2-143	SH-INS-LOSS-VAR-DEG-HIGH, page 2-210
DATAFLT, page 2-66	LOS (ISC), page 2-144	SH-INS-LOSS-VAR-DEG-LOW, page 2-210
DBOSYNC, page 2-66	LOS (FUDC), page 2-143	SHUTTER-OPEN, page 2-210
DS3-MISM, page 2-67	LOS (MSUDC), page 2-144	SIGLOSS, page 2-211
DSP-COMM-FAIL, page 2-68	LOS (OCN), page 2-144	SNTP-HOST, page 2-211
DSP-FAIL, page 2-68	LOS (OTS), page 2-146	SPAN-SW-EAST, page 2-212
DUP-IPADDR, page 2-68	LOS (TRUNK), page 2-147	SPAN-SW-WEST, page 2-212
DUP-NODENAME, page 2-69	LOS-O, page 2-148	SQUELCH, page 2-212
EHIBATVG, page 2-69	LOS-P (OCH, OMS, OTS), page 2-150	SQUELCHED, page 2-214
ELWBATVG, page 2-70	LOS-P (TRUNK), page 2-151	SQM, page 2-215
EOC, page 2-72	LO-TXPOWER, page 2-152	SSM-DUS, page 2-215
EOC-L, page 2-74	LPBKCRS, page 2-153	SSM-FAIL, page 2-215
EQPT, page 2-75	LPBKDS1FEAC, page 2-153	SSM-LNC, page 2-216
EQPT-MISS, page 2-76	LPBKDS1FEAC-CMD, page 2-154	SSM-OFF, page 2-216
ERFI-P-CONN, page 2-76	LPBKDS3FEAC, page 2-154	SSM-PRC, page 2-216
ERFI-P-PAYLD, page 2-76	LPBKDS3FEAC-CMD, page 2-155	SSM-PRS, page 2-217
ERFI-P-SRVR, page 2-77	LPBKFACILITY (TRUNK), page 2-155	SSM-RES, page 2-217
ERROR-CONFIG, page 2-77	LPBKFACILITY(DS1, DS3), page 2-155	SSM-SDN-TN, page 2-217
ETH-LINKLOSS, page 2-78	LPBKFACILITY (EC1-12), page 2-156	SSM-SETS, page 2-217

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

FE-MANWKSWPR-RING, page 2-99	MEA (BIC), page 2-167	UNEQ-V, page 2-233
FE-MANWKSWPR-SPAN, page 2-100	MEA (EQPT), page 2-168	UNREACHABLE-TARGET-POWER, page 2-234
FEPRLF, page 2-100	MEA (FAN), page 2-170	UT-COMM-FAIL, page 2-234
FIBERTEMP-DEG, page 2-101	MEA (PPM), page 2-171	UT-FAIL, page 2-235
FORCED-REQ, page 2-101	MEM-GONE, page 2-172	VCG-DEG, page 2-235
FORCED-REQ-RING, page 2-102	MEM-LOW, page 2-172	VCG-DOWN, page 2-235
FORCED-REQ-SPAN, page 2-102	MFGMEM, page 2-172	VOA-HDEG, page 2-236
FRCDSWTOINT, page 2-102	NO-CONFIG, page 2-173	VOA-HFAIL, page 2-236
FRCDSWTOPRI, page 2-103	OCHNC-INC, page 2-174	VOA-LDEG, page 2-237
FRCDSWTOSEC, page 2-103	ODUK-1-AIS-PM, page 2-174	VOA-LFAIL, page 2-237
FRCDSWTOTHIRD, page 2-103	ODUK-2-AIS-PM, page 2-174	WKSWPR, page 2-237
FRNGSYNC, page 2-103	ODUK-3-AIS-PM, page 2-175	WTR, page 2-238
FSTSYNC, page 2-104	ODUK-4-AIS-PM, page 2-175	WVL-MISMATCH, page 2-238

2.3 Alarm Logical Objects

The CTC alarm profile list organizes all alarms and conditions according to the logical objects they are raised against. These logical objects represent physical objects such as cards, logical objects such as circuits, or transport and signal monitoring entities such as the SONET or ITU-T G.709 optical overhead bits. One alarm might appear in multiple entries when it can be raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the optical signal (OC-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both OCN::LOS and OTN::LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in Table 2-7.

Note Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. For example, the "OCN" logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Table 2-7 Alarm Logical Object Type Definition

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface Controller–International/alarm expansion panel. A combination term that refers to this platform's AIC card.
AIP	Auxiliary interface protection module.
AOTS	Amplified optical transport section.
BIC	Backplane interface connector.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).

Table 2-7 Alarm Logical Object Type Definition (continued)

Logical Object	Definition
BPLANE	The backplane.
DS1	A DS-1 line on a DS-1 or DS-3 electrical card (DS1-14, DS1N-14, DS3-12, DS3N-12, DS3-12E, DS3N-12E, DS3XM-6, DS3XM-12).
DS3	A DS-3 line on a DS-3 electrical card.
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
EC1-12	An EC1-12 electrical card.
ENV	An environmental alarm port.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the eight non-common card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, STS, and VT.
ESCON	Enterprise System Connection fiber optic technology, referring to the following transponder (TXP) cards: TXP_MR_2.5G, TXPP_MR_2.5G.
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E.
FCMR	An FC_MR-4 Fibre Channel card.
FICON	Fiber Connection fiber optic technology, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G.
FUDC	SONET F1 byte user data channel for ONS 15454 ML-Series Ethernet cards.
G1000	A G1000 Ethernet card (G1000-4).
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G.
GFP-FAC	Generic framing procedure facility port, referring to all MXP and TXP cards.
ISC	Inter-service channel, referring to MXP and TXP cards.
ML1000	An ML1000 Ethernet card (ML1000-2).
ML100T	An ML100 card (ML100T-12).
ML2	This object is used in the ONS 15310 platform and is reserved for future use in the ONS 15454 platform.
MSUDC	Multiplex section user data channel.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to Dense Wavelength Division Multiplexer (DWDM) cards. DWDM cards on the ONS 15454 include the OSCM, OSC-CSM, OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.x,AD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the 32WSS.
OCHNC_CONN	The optical channel connection, referring to DWDM cards.

Table 2-7 Alarm Logical Object Type Definition (continued)

Logical Object	Definition
OCN	An OC-N line on any OC-N card.
OMS	Optical multiplex section.
OTS	Optical transport section.
PPM	Pluggable port module, referring to MXP and TXP cards.
STSTRM	STS alarm detection at termination (downstream from the cross-connect).
TRUNK	The optical or dense wavelength division multiplexing (DWDM) card carrying the high-speed signal; referring to MXP or TXP cards.
UCP-CKT	Unified control plane circuit.
UCP-IPCC	Unified control plane IP control channel.
UCP-NBR	Unified control plane neighbor.
VCG	A virtual concatenation group of virtual tributaries (VT).
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect).
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect).

2.4 Alarm Index by Logical Object Type

Table 2-8 lists all ONS 15454 Release 4.7 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Each entry contains a page number that refers to an alarm description in this chapter. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note The list is given here exactly as it is shown in CTC, and in some cases does not follow alphabetical order.

Table 2-8 Alarm Index by Logical Object

2R::ALS, page 2-26	FC::LOCKOUT-REQ, page 2-131	OCN::SQUELCH, page 2-212
2R::AS-CMD, page 2-35	FC::LPBKFACILITY (FC), page 2-157	OCN::SQUELCHED, page 2-214
2R::AS-MT, page 2-36	FC::LPBKTERMINAL (FC), page 2-161	OCN::SSM-DUS, page 2-215
2R::FAILTOSW, page 2-83	FC::MANUAL-REQ-SPAN, page 2-166	OCN::SSM-FAIL, page 2-215
2R::FORCED-REQ-SPAN, page 2-102	FC::OUT-OF-SYNC, page 2-187	OCN::SSM-OFF, page 2-216
2R::HI-LASERBIAS, page 2-112	FC::SIGLOSS, page 2-211	OCN::SSM-PRS, page 2-217
2R::HI-RXPOWER, page 2-114	FC::SQUELCHED, page 2-214	OCN::SSM-RES, page 2-217
2R::HI-TXPOWER, page 2-116	FC::SYNCLOSS, page 2-222	OCN::SSM-SMC, page 2-217
2R::LO-RXPOWER, page 2-138	FC::WKSWPR, page 2-237	OCN::SSM-ST2, page 2-218
2R::LO-TXPOWER, page 2-152	FC::WTR, page 2-238	OCN::SSM-ST3, page 2-218
2R::LOCKOUT-REQ, page 2-131	FCMR::AS-CMD, page 2-35	OCN::SSM-ST3E, page 2-218
2R::LOS (2R), page 2-139	FCMR::AS-MT, page 2-36	OCN::SSM-ST4, page 2-218

Table 2-8 Alarm Index by Logical Object (continued)

2R::MANUAL-REQ-SPAN, page 2-166	FCMR::FC-NO-CREDITS, page 2-89	OCN::SSM-STU, page 2-219
2R::SQUELCHED, page 2-214	FCMR::LPBKFACILITY (FCMR), page 2-157	OCN::SSM-TNC, page 2-219
2R::WKSWPR, page 2-237	FCMR::LPBKTERMINAL (FCMR), page 2-161	OCN::SYNC-FREQ, page 2-222
2R::WTR, page 2-238	FCMR::PORT-MISMATCH, page 2-193	OCN::TIM, page 2-225
AICI-AEP::EQPT, page 2-75	FCMR::SIGLOSS, page 2-211	OCN::TIM-MON, page 2-226
AICI-AEP::MFGMEM, page 2-172	FCMR::SYNCLOSS, page 2-222	OCN::WKSWPR, page 2-237
AICI-AIE::EQPT, page 2-75	FCMR::TPTFAIL (FCMR), page 2-227	OCN::WTR, page 2-238
AICI-AIE::MFGMEM, page 2-172	FUDC::AIS, page 2-24	OMS::APC-CORRECTION-SKIPPED, page 2-26
AIP::INVMACADR, page 2-121	FUDC::LOS (FUDC), page 2-143	OMS::APC-OUT-OF-RANGE, page 2-27
AIP::MEA (AIP), page 2-166	G1000::AS-CMD, page 2-35	OMS::AS-CMD, page 2-35
AIP::MFGMEM, page 2-172	G1000::AS-MT, page 2-36	OMS::AS-MT, page 2-36
AOTS::ALS, page 2-26	G1000::CARLOSS (G1000), page 2-49	OMS::LOS-O, page 2-148
AOTS::AMPLI-INIT, page 2-26	G1000::LPBKFACILITY (G1000), page 2-157	OMS::LOS-P (OCH, OMS, OTS), page 2-150
AOTS::APC-CORRECTION-SKIPPED, page 2-26	G1000::LPBKTERMINAL (G1000), page 2-162	OMS::OPWR-HDEG, page 2-180
AOTS::APC-OUT-OF-RANGE, page 2-27	G1000::TPTFAIL (G1000), page 2-227	OMS::OPWR-HFAIL, page 2-182
AOTS::AS-CMD, page 2-35	GE::ALS, page 2-26	OMS::OPWR-LDEG, page 2-182
AOTS::AS-MT, page 2-36	GE::AS-CMD, page 2-35	OMS::OPWR-LFAIL, page 2-183
AOTS::CASETEMP-DEG, page 2-54	GE::AS-MT, page 2-36	OMS::PARAM-MISM, page 2-187
AOTS::FIBERTEMP-DEG, page 2-101	GE::CARLOSS (GE), page 2-52	OMS::VOA-HDEG, page 2-236
AOTS::GAIN-HDEG, page 2-105	GE::FAILTOSW, page 2-83	OMS::VOA-HFAIL, page 2-236
AOTS::GAIN-HFAIL, page 2-106	GE::FORCED-REQ-SPAN, page 2-102	OMS::VOA-LDEG, page 2-237
AOTS::GAIN-LDEG, page 2-106	GE::GE-OOSYNC, page 2-107	OMS::VOA-LFAIL, page 2-237
AOTS::GAIN-LFAIL, page 2-107	GE::HI-LASERBIAS, page 2-112	OSC-RING::RING-ID-MIS, page 2-201
AOTS::LASER-APR, page 2-125	GE::HI-RXPOWER, page 2-114	OTS::APC-CORRECTION-SKIPPED, page 2-26
AOTS::LASERBIAS-DEG, page 2-125	GE::HI-TXPOWER, page 2-116	OTS::APC-OUT-OF-RANGE, page 2-27
AOTS::LASERBIAS-FAIL, page 2-125	GE::LO-RXPOWER, page 2-138	OTS::AS-CMD, page 2-35
AOTS::LASERTEMP-DEG, page 2-126	GE::LO-TXPOWER, page 2-152	OTS::AS-MT, page 2-36
AOTS::OPWR-HDEG, page 2-180	GE::LOCKOUT-REQ, page 2-131	OTS::AWG-DEG, page 2-43

Table 2-8 Alarm Index by Logical Object (continued)

AOTS::OPWR-HFAIL, page 2-182	GE::LPBKFACILITY (GE), page 2-158	OTS::AWG-FAIL, page 2-43
AOTS::OPWR-LDEG, page 2-182	GE::LPBKTERMINAL (GE), page 2-162	OTS::AWG-OVERTEMP, page 2-43
AOTS::OPWR-LFAIL, page 2-183	GE::MANUAL-REQ-SPAN, page 2-166	OTS::AWG-WARM-UP, page 2-44
AOTS::OSRION, page 2-183	GE::OUT-OF-SYNC, page 2-187	OTS::LASERBIAS-DEG, page 2-125
AOTS::PARAM-MISM, page 2-187	GE::SIGLOSS, page 2-211	OTS::LOS (OTS), page 2-146
AOTS::VOA-HDEG, page 2-236	GE::SQUELCHED, page 2-214	OTS::LOS-O, page 2-148
AOTS::VOA-HFAIL, page 2-236	GE::SYNCLOSS, page 2-222	OTS::LOS-P (OCH, OMS, OTS), page 2-150
AOTS::VOA-LDEG, page 2-237	GE::WKSWPR, page 2-237	OTS::OPWR-HDEG, page 2-180
AOTS::VOA-LFAIL, page 2-237	GE::WTR, page 2-238	OTS::OPWR-HFAIL, page 2-182
BIC::MEA (BIC), page 2-167	GFP-FAC::GFP-CSF, page 2-108	OTS::OPWR-LDEG, page 2-182
BITS::AIS, page 2-24	GFP-FAC::GFP-DE-MISMATCH, page 2-108	OTS::OPWR-LFAIL, page 2-183
BITS::BPV, page 2-46	GFP-FAC::GFP-EX-MISMATCH, page 2-109	OTS::OSRION, page 2-183
BITS::HI-CCVOLT, page 2-112	GFP-FAC::GFP-LFD, page 2-110	OTS::PARAM-MISM, page 2-187
BITS::LOF (BITS), page 2-131	GFP-FAC::GFP-NO-BUFFERS, page 2-110	OTS::SH-INS-LOSS-VAR-DEG-HIGH, page 2-210
BITS::LOS (BITS), page 2-139	GFP-FAC::GFP-UP-MISMATCH, page 2-111	OTS::SH-INS-LOSS-VAR-DEG-LOW, page 2-210
BITS::SSM-DUS, page 2-215	ISC::ALS, page 2-26	OTS::SHUTTER-OPEN, page 2-210
BITS::SSM-FAIL, page 2-215	ISC::AS-CMD, page 2-35	OTS::VOA-HDEG, page 2-236
BITS::SSM-OFF, page 2-216	ISC::AS-MT, page 2-36	OTS::VOA-HFAIL, page 2-236
BITS::SSM-PRS, page 2-217	ISC::CARLOSS (ISC), page 2-52	OTS::VOA-LDEG, page 2-237
BITS::SSM-RES, page 2-217	ISC::FAILTOSW, page 2-83	OTS::VOA-LFAIL, page 2-237
BITS::SSM-SMC, page 2-217	ISC::FORCED-REQ-SPAN, page 2-102	PPM::AS-CMD, page 2-35
BITS::SSM-ST2, page 2-218	ISC::GE-OOSYNC, page 2-107	PPM::AS-MT, page 2-36
BITS::SSM-ST3, page 2-218	ISC::HI-LASERBIAS, page 2-112	PPM::EQPT, page 2-75
BITS::SSM-ST3E, page 2-218	ISC::HI-RXPOWER, page 2-114	PPM::HI-LASERBIAS, page 2-112
BITS::SSM-ST4, page 2-218	ISC::HI-TXPOWER, page 2-116	PPM::HI-LASERTEMP, page 2-113
BITS::SSM-STU, page 2-219	ISC::LO-RXPOWER, page 2-138	PPM::HI-TXPOWER, page 2-116
BITS::SSM-TNC, page 2-219	ISC::LO-TXPOWER, page 2-152	PPM::IMPROPRMVL, page 2-118
BITS::SYNC-FREQ, page 2-222	ISC::LOCKOUT-REQ, page 2-131	PPM::LO-TXPOWER, page 2-152
BPLANE::AS-CMD, page 2-35	ISC::LOS (ISC), page 2-144	PPM::MEA (PPM), page 2-171
BPLANE::MFGMEM, page 2-172	ISC::LPBKFACILITY (ISC), page 2-158	PPM::MFGMEM, page 2-172
DS1::AIS, page 2-24	ISC::LPBKTERMINAL (ISC), page 2-163	PWR::AS-CMD, page 2-35
DS1::AS-CMD, page 2-35	ISC::MANUAL-REQ-SPAN, page 2-166	PWR::BAT-FAIL, page 2-44

Table 2-8 Alarm Index by Logical Object (continued)

DS1::AS-MT, page 2-36	ISC::OUT-OF-SYNC, page 2-187	PWR::EHIBATVG, page 2-69
DS1::LOF (DS1), page 2-132	ISC::SIGLOSS, page 2-211	PWR::ELWBATVG, page 2-70
DS1::LOS (DS1), page 2-140	ISC::SQUELCHED, page 2-214	PWR::HIBATVG, page 2-112
DS1::LPBKDS1FEAC, page 2-153	ISC::SYNCLOSS, page 2-222	PWR::LWBATVG, page 2-164
DS1::LPBKDS1FEAC-CMD, page 2-154	ISC::WKSWPR, page 2-237	STSMON::AIS-P, page 2-25
DS1::LPBKFACILITY(DS1, DS3), page 2-155	ISC::WTR, page 2-238	STSMON::AUTOSW-AIS, page 2-40
DS1::LPBKTERMINAL (DS1, DS3), page 2-160	ML1000::AS-CMD, page 2-35	STSMON::AUTOSW-LOP (STSMON), page 2-40
DS1::RAI, page 2-197	ML1000::AS-MT, page 2-36	STSMON::AUTOSW-PDI, page 2-41
DS1::RCVR-MISS, page 2-198	ML1000::CARLOSS (ML100T, ML1000, ML2), page 2-53	STSMON::AUTOSW-SDBER, page 2-41
DS1::SD (DS1, DS3), page 2-203	ML1000::GFP-CSF, page 2-108	STSMON::AUTOSW-SFBER, page 2-42
DS1::SF (DS1, DS3), page 2-207	ML1000::GFP-DE-MISMATCH, page 2-108	STSMON::AUTOSW-UNEQ (STSMON), page 2-42
DS1::SSM-DUS, page 2-215	ML1000::GFP-EX-MISMATCH, page 2-109	STSMON::ERFI-P-CONN, page 2-76
DS1::SSM-FAIL, page 2-215	ML1000::GFP-LFD, page 2-110	STSMON::ERFI-P-PAYLD, page 2-76
DS1::SSM-OFF, page 2-216	ML1000::GFP-NO-BUFFERS, page 2-110	STSMON::ERFI-P-SRVR, page 2-77
DS1::SSM-PRS, page 2-217	ML1000::GFP-UP-MISMATCH, page 2-111	STSMON::FAILTOSW-PATH, page 2-84
DS1::SSM-RES, page 2-217	ML1000::TPTFAIL (ML1000, ML100T, ML2), page 2-228	STSMON::FORCED-REQ, page 2-101
DS1::SSM-SMC, page 2-217	ML100T::AS-CMD, page 2-35	STSMON::LOCKOUT-REQ, page 2-131
DS1::SSM-ST2, page 2-218	ML100T::AS-MT, page 2-36	STSMON::LOP-P, page 2-136
DS1::SSM-ST3, page 2-218	ML100T::CARLOSS (ML100T, ML1000, ML2), page 2-53	STSMON::LPBKCRS, page 2-153
DS1::SSM-ST3E, page 2-218	ML100T::GFP-CSF, page 2-108	STSMON::MAN-REQ, page 2-164
DS1::SSM-ST4, page 2-218	ML100T::GFP-DE-MISMATCH, page 2-108	STSMON::PDI-P, page 2-188
DS1::SSM-STU, page 2-219	ML100T::GFP-EX-MISMATCH, page 2-109	STSMON::PLM-P, page 2-190
DS1::SSM-TNC, page 2-219	ML100T::GFP-LFD, page 2-110	STSMON::RFI-P, page 2-199
DS1::SYNC-FREQ, page 2-222	ML100T::GFP-NO-BUFFERS, page 2-110	STSMON::SD-P, page 2-206
DS1::TRMT, page 2-229	ML100T::GFP-UP-MISMATCH, page 2-111	STSMON::SF-P, page 2-209
DS1::TRMT-MISS, page 2-230	ML100T::TPTFAIL (ML1000, ML100T, ML2), page 2-228	STSMON::TIM-P, page 2-226

Table 2-8 Alarm Index by Logical Object (continued)

DS1::TX-AIS, page 2-230	ML2::AS-CMD, page 2-35	STSMON::UNEQ-P, page 2-231
DS1::TX-RAI, page 2-230	ML2::AS-MT, page 2-36	STSMON::WKSWPR, page 2-237
DS3::AIS, page 2-24	ML2::CARLOSS (ML100T, ML1000, ML2), page 2-53	STSMON::WTR, page 2-238
DS3::AS-CMD, page 2-35	ML2::GFP-CSF, page 2-108	STSTRM::AIS-P, page 2-25
DS3::AS-MT, page 2-36	ML2::GFP-LFD, page 2-110	STSTRM::AS-MT-OOG, page 2-36
DS3::DS3-MISM, page 2-67	ML2::LPBKFACILITY (ML2), page 2-159	STSTRM::AU-LOF, page 2-38
DS3::FE-AIS, page 2-90	ML2::LPBKTERMINAL (ML2), page 2-163	STSTRM::ENCAP-MISMATCH-P, page 2-70
DS3::FE-DS1-MULTLOS, page 2-91	ML2::TPTFAIL (ML1000, ML100T, ML2), page 2-228	STSTRM::ERFI-P-CONN, page 2-76
DS3::FE-DS1-NSA, page 2-92	MSUDC::AIS, page 2-24	STSTRM::ERFI-P-PAYLD, page 2-76
DS3::FE-DS1-SA, page 2-92	MSUDC::LOS (MSUDC), page 2-144	STSTRM::ERFI-P-SRVR, page 2-77
DS3::FE-DS1-SNGLLOS, page 2-93	NE-SREF::FRCDSWTOINT, page 2-102	STSTRM::LCAS-CRC, page 2-127
DS3::FE-DS3-NSA, page 2-93	NE-SREF::FRCDSWTOPRI, page 2-103	STSTRM::LCAS-RX-FAIL, page 2-128
DS3::FE-DS3-SA, page 2-94	NE-SREF::FRCDSWTOSEC, page 2-103	STSTRM::LCAS-TX-ADD, page 2-128
DS3::FE-EQPT-NSA, page 2-94	NE-SREF::FRCDSWTOTHIRD, page 2-103	STSTRM::LCAS-TX-DNU, page 2-129
DS3::FE-IDLE, page 2-97	NE-SREF::FRNGSYNC, page 2-103	STSTRM::LOM, page 2-136
DS3::FE-LOF, page 2-98	NE-SREF::FSTSYNC, page 2-104	STSTRM::LOP-P, page 2-136
DS3::FE-LOS, page 2-98	NE-SREF::HLDOVRSYNC, page 2-116	STSTRM::OOU-TPT, page 2-179
DS3::INC-ISD, page 2-119	NE-SREF::MANSWTOINT, page 2-165	STSTRM::PDI-P, page 2-188
DS3::LOF (DS3), page 2-133	NE-SREF::MANSWTOPRI, page 2-165	STSTRM::PLM-P, page 2-190
DS3::LOS (DS3), page 2-141	NE-SREF::MANSWTOSEC, page 2-165	STSTRM::RFI-P, page 2-199
DS3::LPBKDS1FEAC, page 2-153	NE-SREF::MANSWTOTHIRD, page 2-165	STSTRM::SD-P, page 2-206
DS3::LPBKDS3FEAC, page 2-154	NE-SREF::SSM-PRS, page 2-217	STSTRM::SF-P, page 2-209
DS3::LPBKDS3FEAC-CMD, page 2-155	NE-SREF::SSM-RES, page 2-217	STSTRM::SQM, page 2-215
DS3::LPBKFACILITY(DS1, DS3), page 2-155	NE-SREF::SSM-SMC, page 2-217	STSTRM::TIM-P, page 2-226
DS3::LPBKTERMINAL (DS1, DS3), page 2-160	NE-SREF::SSM-ST2, page 2-218	STSTRM::UNEQ-P, page 2-231
DS3::RAI, page 2-197	NE-SREF::SSM-ST3, page 2-218	TRUNK::AIS, page 2-24
DS3::SD (DS1, DS3), page 2-203	NE-SREF::SSM-ST3E, page 2-218	TRUNK::ALS, page 2-26
DS3::SF (DS1, DS3), page 2-207	NE-SREF::SSM-ST4, page 2-218	TRUNK::AS-CMD, page 2-35
E1000F::AS-CMD, page 2-35	NE-SREF::SSM-STU, page 2-219	TRUNK::AS-MT, page 2-36

Table 2-8 Alarm Index by Logical Object (continued)

E1000F::CARLOSS (E100T, E1000F), page 2-46	NE-SREF::SSM-TNC, page 2-219	TRUNK::CARLOSS (TRUNK), page 2-54
E100T::AS-CMD, page 2-35	NE-SREF::SWTOPRI, page 2-221	TRUNK::DSP-COMM-FAIL, page 2-68
E100T::CARLOSS (E100T, E1000F), page 2-46	NE-SREF::SWTOSEC, page 2-221	TRUNK::DSP-FAIL, page 2-68
EC1-12::AIS-L, page 2-24	NE-SREF::SWTOTHIRD, page 2-221	TRUNK::EOC, page 2-72
EC1-12::AS-CMD, page 2-35	NE-SREF::SYNCPRI, page 2-223	TRUNK::EOC-L, page 2-74
EC1-12::AS-MT, page 2-36	NE-SREF::SYNCSEC, page 2-223	TRUNK::FAILTOSW, page 2-83
EC1-12::FE-FRCDWKSWBK-SPAN , page 2-95	NE-SREF::SYNCTHIRD, page 2-224	TRUNK::FEC-MISM, page 2-91
EC1-12::FE-MANWKSWBK-SPAN, page 2-99	NE::APC-DISABLED, page 2-27	TRUNK::FORCED-REQ-SPAN, page 2-102
EC1-12::HELLO, page 2-111	NE::APC-END, page 2-27	TRUNK::GCC-EOC, page 2-107
EC1-12::HI-LASERTEMP, page 2-113	NE::AS-CMD, page 2-35	TRUNK::GE-OOSYNC, page 2-107
EC1-12::LO-LASERTEMP, page 2-135	NE::AUD-LOG-LOSS, page 2-37	TRUNK::HI-LASERBIAS, page 2-112
EC1-12::LOF (EC1-12), page 2-134	NE::AUD-LOG-LOW, page 2-37	TRUNK::HI-RXPOWER, page 2-114
EC1-12::LOS (EC1-12), page 2-141	NE::DATAFLT, page 2-66	TRUNK::HI-TXPOWER, page 2-116
EC1-12::LPBKFACILITY (EC1-12), page 2-156	NE::DBOSYNC, page 2-66	TRUNK::LO-RXPOWER, page 2-138
EC1-12::LPBKTERMINAL (EC1-12), page 2-160	NE::DUP-IPADDR, page 2-68	TRUNK::LO-TXPOWER, page 2-152
EC1-12::RFI-L, page 2-199	NE::DUP-NODENAME, page 2-69	TRUNK::LOCKOUT-REQ, page 2-131
EC1-12::SD-L, page 2-205	NE::ETH-LINKLOSS, page 2-78	TRUNK::LOF (TRUNK), page 2-135
EC1-12::SF-L, page 2-208	NE::HITEMP, page 2-115	TRUNK::LOM, page 2-136
EC1-12::SQUELCHED, page 2-214	NE::I-HITEMP, page 2-117	TRUNK::LOS (TRUNK), page 2-147
EC1-12::TIM-MON, page 2-226	NE::INTRUSION-PSWD, page 2-121	TRUNK::LOS-P (TRUNK), page 2-151
ENVALRM::EXT, page 2-82	NE::LAN-POL-REV, page 2-124	TRUNK::LPBKFACILITY (TRUNK), page 2-155
EQPT::AS-CMD, page 2-35	NE::OPTNTWMIS, page 2-179	TRUNK::LPBKTERMINAL (TRUNK), page 2-159
EQPT::AS-MT, page 2-36	NE::SNTP-HOST, page 2-211	TRUNK::MANUAL-REQ-SPAN, page 2-166
EQPT::AUTORESET, page 2-39	NE::SYSBOOT, page 2-225	TRUNK::ODUK-AIS-PM, page 2-176
EQPT::BKUPMEMP, page 2-45	OCH::AS-CMD, page 2-35	TRUNK::ODUK-2-AIS-PM, page 2-174
EQPT::CARLOSS (EQPT), page 2-48	OCH::AS-MT, page 2-36	TRUNK::ODUK-3-AIS-PM, page 2-175
EQPT::CLDRESTART, page 2-57	OCH::LOS-O, page 2-148	TRUNK::ODUK-4-AIS-PM, page 2-175
EQPT::COMIOXC, page 2-58	OCH::LOS-P (OCH, OMS, OTS), page 2-150	TRUNK::ODUK-BDI-PM, page 2-176

Table 2-8 Alarm Index by Logical Object (continued)

EQPT::COMM-FAIL, page 2-58	OCH::OPWR-HDEG, page 2-180	TRUNK::ODUK-LCK-PM, page 2-177
EQPT::CONTBUS-A-18, page 2-59	OCH::OPWR-HFAIL, page 2-182	TRUNK::ODUK-OCI-PM, page 2-177
EQPT::CONTBUS-B-18, page 2-60	OCH::OPWR-LDEG, page 2-182	TRUNK::ODUK-SD-PM, page 2-178
EQPT::CONTBUS-IO-A, page 2-60	OCH::OPWR-LFAIL, page 2-183	TRUNK::ODUK-SF-PM, page 2-178
EQPT::CONTBUS-IO-B, page 2-61	OCH::PARAM-MISM, page 2-187	TRUNK::ODUK-TIM-PM, page 2-179
EQPT::CTNEQPT-MISMATCH, page 2-62	OCH::PORT-ADD-PWR-DEG-HI, page 2-191	TRUNK::OTUK-AIS, page 2-183
EQPT::CTNEQPT-PBPROT, page 2-63	OCH::PORT-ADD-PWR-DEG-LOW, page 2-191	TRUNK::OTUK-BDI, page 2-184
EQPT::CTNEQPT-PBWORK, page 2-65	PORT-ADD-PWR-FAIL-HI, page 2-191	TRUNK::OTUK-IAE, page 2-185
EQPT::EQPT, page 2-75	OCH::PORT-ADD-PWR-FAIL-LOW, page 2-192	TRUNK::OTUK-LOF, page 2-185
EQPT::ERROR-CONFIG, page 2-77	OCH::UNREACHABLE-TARGET-POWER, page 2-234	TRUNK::OTUK-SD, page 2-185
EQPT::EXCCOL, page 2-81	OCH::VOA-HDEG, page 2-236	TRUNK::OTUK-SD, page 2-185
EQPT::FAILTOSW, page 2-83	OCH::VOA-HFAIL, page 2-236	TRUNK::OTUK-TIM, page 2-186
EQPT::FORCED-REQ, page 2-101	OCH::VOA-LDEG, page 2-237	TRUNK::OUT-OF-SYNC, page 2-187
EQPT::HITEMP, page 2-115	OCH::VOA-LFAIL, page 2-237	TRUNK::PTIM, page 2-194
EQPT::IMPROPRMVL, page 2-118	OCHNC-CONN::OCHNC-INC, page 2-174	TRUNK::RFI, page 2-198
EQPT::INHSWPR, page 2-120	OCN::AIS-L, page 2-24	TRUNK::SD (TRUNK), page 2-203
EQPT::INHSWWKG, page 2-120	OCN::ALS, page 2-26	TRUNK::SF (TRUNK), page 2-207
EQPT::IOSCFGCOPY, page 2-123	OCN::APS-INV-PRIM, page 2-33	TRUNK::SIGLOSS, page 2-211
EQPT::LOCKOUT-REQ, page 2-131	OCN::APS-PRIM-FAC, page 2-33	TRUNK::SQUELCHED, page 2-214
EQPT::MAN-REQ, page 2-164	OCN::APS-PRIM-SEC-MISM, page 2-34	TRUNK::SSM-DUS, page 2-215
EQPT::MANRESET, page 2-164	OCN::APSB, page 2-28	TRUNK::SSM-FAIL, page 2-215
EQPT::MEA (EQPT), page 2-168	OCN::APSCDFLTK, page 2-29	TRUNK::SSM-LNC, page 2-216
EQPT::MEM-GONE, page 2-172	OCN::APSC-IMP, page 2-29	TRUNK::SSM-OFF, page 2-216
EQPT::MEM-LOW, page 2-172	OCN::APSCINCON, page 2-30	TRUNK::SSM-PRC, page 2-216
EQPT::NO-CONFIG, page 2-173	OCN::APSCM, page 2-31	TRUNK::SSM-PRS, page 2-217
EQPT::PEER-NORESPONSE, page 2-189	OCN::APSCNMIS, page 2-32	TRUNK::SSM-RES, page 2-217
EQPT::PROTNA, page 2-194	OCN::APSIMP, page 2-32	TRUNK::SSM-SDN-TN, page 2-217
EQPT::PWR-FAIL-A, page 2-195	OCN::APSMM, page 2-34	TRUNK::SSM-SETS, page 2-217
EQPT::PWR-FAIL-B, page 2-196	OCN::AS-CMD, page 2-35	TRUNK::SSM-SMC, page 2-217
EQPT::PWR-FAIL-RET-A, page 2-196	OCN::AS-MT, page 2-36	TRUNK::SSM-ST2, page 2-218

Table 2-8 Alarm Index by Logical Object (continued)

EQPT::PWR-FAIL-RET-B, page 2-197	OCN::AUTOLSROFF, page 2-38	TRUNK::SSM-ST3, page 2-218
EQPT::RUNCFG-SAVENEED, page 2-203	OCN::BLSROSYNC, page 2-45	TRUNK::SSM-ST3E, page 2-218
EQPT::SFTWDOWN, page 2-209	OCN::E-W-MISMATCH, page 2-79	TRUNK::SSM-ST4, page 2-218
EQPT::SWMTXMOD, page 2-219	OCN::EOC, page 2-72	TRUNK::SSM-STU, page 2-219
EQPT::WKSWPR, page 2-237	OCN::EOC-L, page 2-74	TRUNK::SSM-TNC, page 2-219
EQPT::WTR, page 2-238	OCN::EXERCISE-RING-FAIL, page 2-81	TRUNK::SYNC-FREQ, page 2-222
ESCON::ALS, page 2-26	OCN::EXERCISE-SPAN-FAIL, page 2-82	TRUNK::SYNCLOSS, page 2-222
ESCON::AS-CMD, page 2-35	OCN::EXTRA-TRAF-PREEMPT, page 2-83	TRUNK::TIM, page 2-225
ESCON::AS-MT, page 2-36	OCN::FAILTOSW, page 2-83	TRUNK::TIM-MON, page 2-226
ESCON::FAILTOSW, page 2-83	OCN::FAILTOSWR, page 2-85	TRUNK::UNC-WORD, page 2-231
ESCON::FORCED-REQ-SPAN, page 2-102	OCN::FAILTOSWS, page 2-87	TRUNK::UT-COMM-FAIL, page 2-234
ESCON::HI-LASERBIAS, page 2-112	OCN::FE-FRCDWKSWBK-SPAN, page 2-95	TRUNK::UT-FAIL, page 2-235
ESCON::HI-RXPOWER, page 2-114	OCN::FE-FRCDWKSWPR-RING, page 2-96	TRUNK::WKSWPR, page 2-237
ESCON::HI-TXPOWER, page 2-116	OCN::FE-FRCDWKSWPR-SPAN, page 2-96	TRUNK::WTR, page 2-238
ESCON::LO-RXPOWER, page 2-138	OCN::FE-LOCKOUTOFPR-SPAN, page 2-97	TRUNK::WVL-MISMATCH, page 2-238
ESCON::LO-TXPOWER, page 2-152	OCN::FE-MANWKSWBK-SPAN, page 2-99	UCP-CKT::CKTDOWN, page 2-55
ESCON::LOCKOUT-REQ, page 2-131	OCN::FE-MANWKSWPR-RING, page 2-99	UCP-IPCC::LMP-HELLODOWN, page 2-130
ESCON:: LOS (ESCON), page 2-143	OCN::FE-MANWKSWPR-SPAN, page 2-100	UCP-IPCC::LMP-NDFAIL, page 2-130
ESCON::LPBKFACILITY (ESCON), page 2-156	OCN::FEPRLF, page 2-100	UCP-NBR::RSVP-HELLODOWN, page 2-202
ESCON::LPBKTERMINAL (ESCON), page 2-161	OCN::FORCED-REQ-RING, page 2-102	VCG::LOA, page 2-130
ESCON::MANUAL-REQ-SPAN, page 2-166	OCN::FORCED-REQ-SPAN, page 2-102	VCG::VCG-DEG, page 2-235
ESCON::SQUELCHED, page 2-214	OCN::FULLPASSTHR-BI, page 2-104	VCG::VCG-DOWN, page 2-235
ESCON::WKSWPR, page 2-237	OCN::HELLO, page 2-111	VT-MON::AIS-V, page 2-25
ESCON::WTR, page 2-238	OCN::HI-LASERBIAS, page 2-112	VT-MON::AUTOSW-AIS, page 2-40
EXT-SREF::FRCDSWTOPRI, page 2-103	OCN::HI-LASERTEMP, page 2-113	VT-MON::AUTOSW-LOP (VT-MON), page 2-41

Table 2-8 Alarm Index by Logical Object (continued)

EXT-SREF::FRCDSWTOSEC, page 2-103	OCN::HI-RXPOWER, page 2-114	VT-MON::AUTOSW-UNEQ (VT-MON), page 2-42
EXT-SREF::FRCDSWTOTHIRD, page 2-103	OCN::HI-TXPOWER, page 2-116	VT-MON::FAILTOSW-PATH, page 2-84
EXT-SREF::MANSWTOPRI, page 2-165	OCN::KB-PASSTHR, page 2-123	VT-MON::FORCED-REQ, page 2-101
EXT-SREF::MANSWTOSEC, page 2-165	OCN::KBYTE-APS-CHANNEL-FAILURE, page 2-124	VT-MON::LOCKOUT-REQ, page 2-131
EXT-SREF::MANSWTOTHIRD, page 2-165	OCN::LASEREOL, page 2-126	VT-MON::LOP-V, page 2-137
EXT-SREF::SWTOPRI, page 2-221	OCN::LKOUTPR-S, page 2-129	VT-MON::MAN-REQ, page 2-164
EXT-SREF::SWTOSEC, page 2-221	OCN::LO-LASERTEMP, page 2-135	VT-MON::SD-V, page 2-206
EXT-SREF::SWTOTHIRD, page 2-221	OCN::LO-RXPOWER, page 2-138	VT-MON::SF-V, page 2-209
EXT-SREF::SYNCPRI, page 2-223	OCN::LO-TXPOWER, page 2-152	VT-MON::UNEQ-V, page 2-233
EXT-SREF::SYNCSEC, page 2-223	OCN::LOCKOUT-REQ, page 2-131	VT-MON::WKSWPR, page 2-237
EXT-SREF::SYNCTHIRD, page 2-224	OCN::LOF (OCN), page 2-134	VT-MON::WTR, page 2-238
FAN::EQPT-MISS, page 2-76	OCN::LOS (OCN), page 2-144	VT-TERM::AIS-V, page 2-25
FAN::FAN, page 2-89	OCN::LPBKFACILITY (OCN), page 2-159	VT-TERM::AS-MT-OOG, page 2-36
FAN::MEA (FAN), page 2-170	OCN::LPBKTERMINAL (OCN), page 2-163	VT-TERM::LCAS-CRC, page 2-127
FAN::MFGMEM, page 2-172	OCN::MANUAL-REQ-RING, page 2-166	VT-TERM::LCAS-RX-FAIL, page 2-128
FC::ALS, page 2-26	OCN::MANUAL-REQ-SPAN, page 2-166	VT-TERM::LCAS-TX-ADD, page 2-128
FC::AS-CMD, page 2-35	OCN::PRC-DUPID, page 2-193	VT-TERM::LCAS-TX-DNU, page 2-129
FC::AS-MT, page 2-36	OCN::RFI-L, page 2-199	VT-TERM::LOM, page 2-136
FC::CARLOSS (FC), page 2-49	OCN::RING-ID-MIS, page 2-201	VT-TERM::LOP-V, page 2-137
FC::FAILTOSW, page 2-83	OCN::RING-MISMATCH, page 2-201	VT-TERM::OOU-TPT, page 2-179
FC::FORCED-REQ-SPAN, page 2-102	OCN::RING-SW-EAST, page 2-202	VT-TERM::PLM-V, page 2-191
FC::GE-OOSYNC, page 2-107	OCN::RING-SW-WEST, page 2-202	VT-TERM::RFI-V, page 2-200
FC::HI-LASERBIAS, page 2-112	OCN::SD-L, page 2-205	VT-TERM::SD-P, page 2-206
FC::HI-RXPOWER, page 2-114	OCN::SF-L, page 2-208	VT-TERM::SF-P, page 2-209
FC::HI-TXPOWER, page 2-116	OCN::SPAN-SW-EAST, page 2-212	VT-TERM::SQM, page 2-215
FC::LO-RXPOWER, page 2-138	OCN::SPAN-SW-WEST, page 2-212	VT-TERM::UNEQ-V, page 2-233
FC::LO-TXPOWER, page 2-152	—	—

2.5 DS3-12 E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M13, or C Bit. The choice of framing format determines the line alarms that the DS3-12E card reports. The following table lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms and conditions, listed in Table 2-9, as the standard DS-3 card reports.

Table 2-9 DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS (DS1), LOS (DS3)	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF (DS1), LOF (DS3)	No	Yes	Yes
FE-IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk (LPBKTERMINAL (DS1, DS3)	Yes	Yes	Yes
Facility Lpbk (LPBKFACILITY(DS1, DS3)	Yes	Yes	Yes
FE Lpbk (LPBKDS1FEAC, LPBKDS3FEAC)	No	No	Yes
FE Common Equipment Failure (FE-DS1-NSA, FE-DS3-NSA)	No	No	Yes
FE Equipment Failure-SA (FE-DS3-SA)	No	No	Yes
FE-LOS	No	No	Yes
FE-LOF	No	No	Yes
FE-AIS	No	No	Yes
FE-IDLE	No	No	Yes
FE Equipment Failure-NSA (FE-EQPT-NSA)	No	No	Yes

2.6 Trouble Notifications

The ONS 15454 system reports trouble by utilizing standard alarm and condition characteristics, standard severities following the rules in Telcordia GR-253, and graphical user interface (GUI) state indicators.These notifications are described in the following paragraphs.

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal (LOS). Conditions do not necessarily require troubleshooting.

2.6.1 Alarm Characteristics

The ONS 15454 uses standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are also found in the History tab.)

2.6.2 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are also found in the History tab.)

2.6.3 Severities

The ONS 15454 uses Telcordia-devised standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) and Not Reported (NR):

- A Critical alarm generally indicates severe, service-affecting trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical, but loss of traffic on one to five DS-1 circuits is Major (MJ).
- Minor (MN) alarms generally are those that do not affect service.
- Not Alarmed (NA) conditions are information indicators, such as for state (FRNGSYNC) or an event (FRCSWTOPRI). They might or might not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

All alarm, condition, and not-reported event severities listed in this manual are default profile settings. However in situations when traffic is not lost—such as when the alarm occurs on protected ports or circuits—alarms having Critical (CR) or Major (MJ) default severities can be demoted to lower severities such as Minor (MN) or Non-Service Affecting (NSA) as defined in Telcordia GR-474.

Severities can also be customized for an entire network or for single nodes, down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474.

2.6.4 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—might be Critical (CR), Major (MJ), or Minor (MN) severity alarms. In some cases the severity of an alarm might not correspond to its service effect. For example, the AUTOSW-LOP alarm for the VTMON object is minor but service-affecting because it indicates a traffic switch has occurred directing traffic away from a loss of circuit path. Non-Service Affecting (NSA) alarms always have a Minor (MN) default severity.

2.6.5 States

The Alarms or History tab state (ST) columns indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action.

Note Transient events are not defined in this documentation release.

2.7 Safety Summary

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

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

Some troubleshooting procedures require installation or removal of OC-192 cards; in these instances users should pay close attention to the following warnings.

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

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

Warning **Class 1 laser product.**

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

2.8 Alarm Procedures

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

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

2.8.1 AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, DS3, FUDC, MSUDC, TRUNK

The Alarm Indication Signal (AIS) condition indicates that this node is detecting AIS in the incoming signal SONET overhead.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Note ONS 15454 DS-3 and EC-1 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-144, or out-of-service (OOS,MT or OOS,DSBLD) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1 800 553-2447).

2.8.2 AIS-L

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)

- Logical Objects: EC1-12, OCN

The AIS Line condition indicates that this node is detecting line-level AIS in the incoming signal. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1 800 553-2447).

2.8.3 AIS-P

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

AIS Path condition means that this node is detecting AIS in the incoming path. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1 800 553-2447).

2.8.4 AIS-V

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: VT-MON, VT-TERM

The AIS Virtual Tributary (VT) condition means that this node is detecting AIS in the incoming VT-level path.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

See the "1.8.2 AIS-V on DS3XM-6 Unused VT Circuits" section on page 1-59 for more information.

Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1 800 553-2447).

2.8.5 ALS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition occurs when an Optical Preamplifier (OPT-PRE) or Optical Booster (OPT-BST) amplifier card is switched on. The turn-on process lasts approximately nine seconds, and the condition clears after approximately 10 seconds.

Note ALS is an informational condition and does not require troubleshooting.

2.8.6 AMPLI-INIT

The AMPLI-INIT condition is not used in this platform in this release. It is reserved for future development.

2.8.7 APC-CORRECTION-SKIPPED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OMS, OTS

The Automatic Power Control (APC) Correction Skipped condition occurs when the actual power level of a DWDM channel exceeds the threshold setting by 3 dB or more. The APC compares actual power levels with power level thresholds every 10 minutes or after any channel allocation is performed. If the actual power level is above or below the setting within 3 dB, APC corrects the level. If the actual power level exceeds the threshold by +3 dB or –3 dB, APC cannot correct the level and the APC-CORRECTION-SKIPPED condition is raised.

There is no operator action to resolve this condition. It stays raised until the power level problem is resolved and APC takes a normal reading.

Note APC-CORRECTION-SKIPPED is an informational condition and does not require troubleshooting.

2.8.8 APC-DISABLED

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Disabled alarm occurs when the information related to the number of DWDM channels is not reliable. The alarm can occur when the any related alarms also occur: the "AMPLI-INIT" condition on page 2-26, the "EQPT" alarm on page 2-75, the "IMPROPRMVL" alarm on page 2-118, or the "MEA (EQPT)" alarm on page 2-168. If the alarm occurs with the creation of the first circuit, delete and recreate it.

Clear the APC-DISABLED Alarm

Step 1 Complete the appropriate procedure to clear the main alarm:

- Clear the EQPT Alarm, page 2-75
- Clear the IMPROPRMVL Alarm, page 2-118
- Clear the MEA (EQPT) Alarm, page 2-168

Step 2 If the alarm does not clear, complete the "Delete a Circuit" procedure on page 2-254 and then recreate it using procedures in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.9 APC-END

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Terminated on Manual Request condition is raised when the APC application terminates after being manually launched from CTC or TL1. It is an informational condition.

Note APC-END is an informational condition and does not require troubleshooting.

2.8.10 APC-OUT-OF-RANGE

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OMS, OTS

The APC Out of Range condition is raised on amplifier cards (OPT-PRE and OPT-BST); optical service channel cards (OSCM and OSC-CSM); multiplexer cards (32MUX-O); demultiplexer cards (32DMX, 32DMX-O), and optical add/drop multiplexer cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x) when the requested gain or attenuation setpoint cannot be set because it exceeds the port parameter range.

Clear the APC-OUT-OF-RANGE Condition

Step 1 Provision the correct setpoint. For instructions, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The condition clears when the APC setting is corrected, and APC does not detect any errors in its next cycle.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.11 APSB

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Automatic Protection Switching (APS) Channel Byte Failure alarm occurs when line terminating equipment detects protection switching byte failure or an invalid code in the incoming APS signal. Some older non-Cisco SONET nodes send invalid APS codes if they are configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15454. These invalid codes causes an APSB on an ONS 15454.

Step 1 Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454.

Step 2 If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly. Complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution For the ONS 15454, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used alarm troubleshooting 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 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.12 APSCDFLTK

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Default K Byte Received alarm occurs during bidirectional line switched ring (BLSR) provisioning or when a BLSR is not properly configured, for example, when a four-node BLSR has one node configured as a path protection. When this misconfiguration occurs, a node in a path protection or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for the "BLSROSYNC" alarm on page 2-45.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241 to verify that each node has a unique node ID number.

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

Step 3 If two nodes have the same node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-241 to change one node ID number so that each node ID is unique.

Step 4 If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the "E-W-MISMATCH" alarm on page 2-79.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 DWDM Installation and Operations Guide* provides a procedure for fibering BLSRs.

Step 5 If the alarm does not clear and the network is a four-fiber BLSR, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protection fiber.

Step 6 If the alarm does not clear, complete the "Verify Node Visibility for Other Nodes" procedure on page 2-242.

Step 7 If nodes are not visible, complete the "Verify or Create Node SDCC Terminations" procedure on page 2-254 to ensure that SONET data communications channel (SDCC) terminations exist on each node.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.13 APSC-IMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

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

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

Note This alarm can occur on a virtual tributary (VT) tunnel when it does not have VT circuits provisioned. It can also occur when the exercise command or a lockout is applied to a span. An externally switched span does not raise this alarm because traffic is preempted.

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

Clear the APSC-IMP Alarm

Step 1 Use an optical test set to determine the validity of the K byte signal by examining the received signal. For specific procedures to use the test set equipment, consult the manufacturer.

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

Step 2 If the K byte is valid, verify that each node has a ring name that matches the other node ring names. Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241.

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

Step 4 If a node has a ring name that does not match the other nodes, make the ring name of that node identical to the other nodes. Complete the "Change a BLSR Ring Name" procedure on page 2-241.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.14 APSCINCON

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

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

Clear the APSCINCON Alarm

Step 1 Look for other alarms, especially the "LOS (OCN)" alarm on page 2-144, the "LOF (OCN)" alarm on page 2-134, or the "AIS" alarm on page 2-24. Clearing these alarms clears the APSCINCON alarm.

Step 2 If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.15 APSCM

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

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 does not occur. The APSCM alarm occurs only on the ONS 15454 when bidirectional protection is used on OC-N cards in a 1+1 configuration.

Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service (IS-NR) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

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

Clear the APSCM Alarm

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

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node protection-card channel fibers.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.16 APSCNMIS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

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

Clear the APSCNMIS Alarm

Step 1 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241 to verify that each node has a unique node ID number.

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

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

Step 4 If two nodes have the same node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-241 to change one node ID number so that each node ID is unique.

Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. The BLSR window shows the node ID of the login node.

Note Applying and removing a lockout on a span causes the ONS node to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

Step 5 If the alarm does not clear, use the "Initiate a Lock Out on a BLSR Protect Span" procedure on page 2-248 to lockout the span.

Step 6 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249 to clear the lockout.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.17 APSIMP

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Invalid Code condition occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for path protection or BLSR protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the proper type of byte.

The condition is superseded by an APS, APSCM, or APSMM. It is not superseded by AIS or remote defect indication (RDI) line alarms. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Condition

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group. For instructions, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Step 3 Ensure that both protect ports are configured for SONET.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.18 APS-INV-PRIM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Primary Facility condition occurs on OC-N cards in an optimized 1+1 protection system if the incoming primary section header does not indicate whether it is primary or secondary.

Note APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

2.8.19 APS-PRIM-FAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Invalid Primary Section condition occurs on OC-N cards in an optimized 1+1 protection system if there is an APS status switch between the primary and secondary facilities to identify which port is primary.

Note APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

Clear the APS-PRIM-FAC Condition

Step 1 This condition clears when the card receives a valid primary section indication (1 or 2).

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.20 APSMM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An APS Mode Mismatch failure alarm occurs on OC-N cards when there is a mismatch of the protection switching schemes at the two ends of the span, such as being bidirectional and unidirectional at each end. Each end of a span must be provisioned the same way: bidirectional and bidirectional, or unidirectional and unidirectional. APSMM can also occur if a non-Cisco vendor's equipment is provisioned as 1:N and the ONS 15454 is provisioned as 1+1.

If one end is provisioned for 1+1 protection switching and the other is provisioned for path protection switching, an APSMM alarm occurs in the ONS 15454 that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Step 1 For the reporting ONS 15454, display node view and verify the protection scheme provisioning:

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

b. Click the 1+1 protection group configured for the OC-N cards.

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

c. Click **Edit**.

d. Record whether the Bidirectional Switching check box is checked.

Step 2 Click **OK** in the Edit Protection Group dialog box.

Step 3 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 4 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1. If not, change it to match.

Step 5 Click **Apply**.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.21 APS-PRIM-SEC-MISM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Primary Section Mismatch condition occurs on OC-N cards in an optimized 1+1 protection system if there is a match between the primary section of the near end facility and the primary section of the far-end facility.

Clear the APS-PRIM-SEC-MISM Alarm

Step 1 Ensure that the near end and far-end ports are correctly provisioned with the same way. For more information about optimized 1+1 configurations, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.22 AS-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, BPLANE, DS1, DS3, E1000F, E100T, EC1-12, EQPT, ESCON, FC, ML2, NE, OCH, OCN, OMS, OTS, PPM, PWR, TRUNK

The Alarms Suppressed by User Command condition applies to the network element (NE object), backplane, a single card, or a port on a card. It occurs when alarms are suppressed for that object and its subordinate objects. Suppressing alarms on a card also suppresses alarms on its ports.

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the AS-CMD Condition

Step 1 For all nodes, in node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column, and note what entity the condition is reported against, such as a port, slot, or shelf.

- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.
- If the condition is reported against the backplane, go to Step 7.
- If the condition is reported against the NE object, go to Step 8.

Step 3 Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:

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

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

- If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
- If the Suppress Alarms column check box is not checked for a port row, click **View > Go to Previous View**.

Step 4 If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 5 Locate the row number for the reported card slot.

Step 6 Click the **Suppress Alarms** column check box to deselect the option for the card row.

Step 7 If the condition is reported for the backplane, the alarms are suppressed for cards such as the ONS 15454 AIP that are not in the optical or electrical slots. To clear the alarm:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. In the backplane row, deselect the Suppress Alarms column check box.

c. Click **Apply**.

Step 8 If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

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

c. Click **Apply**.

Step 9 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1 800 553-2447).

2.8.23 AS-MT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, DS1, DS3, EC1-12, EQPT, ESCON, FC, FCMR, G1000, GE, ISC, ML1000, ML100T, ML2, OCH, OCN, OMS, OTS, PPM, TRUNK

The Alarms Suppressed for Maintenance Command condition applies to OC-N and electrical cards and occurs when a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state for loopback testing operations.

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the AS-MT Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-254.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.24 AS-MT-OOG

- Default Severity: Critical (CR), Service-Affecting (SA) if all VCAT members on an STS are placed OOS; Major (MJ), Service-Affecting (SA) for a single VT
- Logical Object: VT-TERM

The Alarms Suppressed on an Out-Of-Group VCAT Member alarm is raised on an STS or VT member of a VCAT group whenever the member is in the IDLE (AS-MT-OOG) admin state. This alarm can be raised when a member is initially added to a group. In IDLE (AS-MT-OOG) state, all other alarms for the STS or VT are suppressed.

Clear the AS-MT-OOG Alarm

Step 1 The AS-MT-OOG alarm clears when an STS or VT member transitions to a different state from IDLE (AS-MT-OOG) or when it is removed completely from the VCAT group. It does not require troubleshooting unless it does not clear.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.25 AUD-LOG-LOSS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Loss condition occurs when the log is 100 percent full and that the oldest entries are being replaced as new entries are generated. The log capacity is 640 entries. The log must be off-loaded using the following procedure to make room for more entries.

Clear the AUD-LOG-LOSS Condition

Step 1 In node view, click the **Maintenance > Audit** tabs.

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not have to assign an extension to the file. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**.

The 640 entries will be saved in this file. New entries will continue with the next number in the sequence, rather than starting over.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.26 AUD-LOG-LOW

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: NE

The Audit Trail Log Low condition occurs when the audit trail log is 80 percent full.

Note AUD-LOG-LOW is an informational condition and does not require troubleshooting.

2.8.27 AU-LOF

The Administrative Unit Loss of Multiframe alarm is not used in this platform in this release. It is reserved for future development.

2.8.28 AUTOLSROFF

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The Auto Laser Shutdown alarm occurs when the OC-192 card temperature exceeds 194 degrees F (90 degrees C). The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.

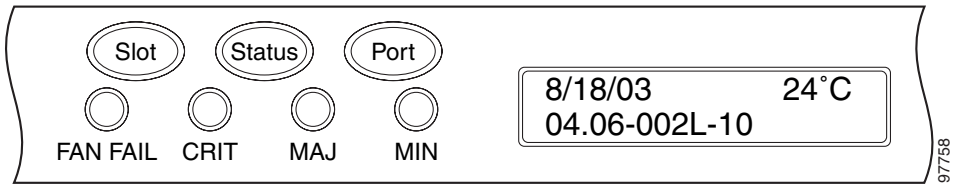
Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service (IS-NR) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

Clear the AUTOLSROFF Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-2).

Figure 2-1 Shelf LCD Panel



Step 2 If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-115.

Step 3 If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the OC-192 card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used troubleshooting 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 4 If card replacement does not clear the alarm, call Cisco TAC (1 800 553-2447) to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

2.8.29 AUTORESET

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

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

AUTORESET typically clears after a card reboots (up to ten minutes). If the alarm does not clear, complete the following procedure.

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 edge of the shelf assembly.

Clear the AUTORESET Alarm

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution For the ONS 15454, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.30 AUTOSW-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The Automatic Path Protection Switch Caused by AIS condition indicates that automatic path protection switching occurred because of an AIS condition. The path protection is configured for revertive switching and reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.31 AUTOSW-LOP (STSMON)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the "LOP-P" alarm on page 2-136. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-137.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.32 AUTOSW-LOP (VT-MON)

- Default Severity: Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

The AUTOSW-LOP alarm for the virtual tributary monitor (VT-MON) indicates that automatic path protection switching occurred because of the "LOP-V" alarm on page 2-137. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (VT-MON) Alarm

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-138.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.33 AUTOSW-PDI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a "PDI-P" alarm on page 2-188. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-188.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.34 AUTOSW-SDBER

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade (SD) caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.35 AUTOSW-SFBER

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal failure (SF) caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF (DS1, DS3) Condition" procedure on page 2-208.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.36 AUTOSW-UNEQ (STSMON)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an UNEQ alarm caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-232.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.37 AUTOSW-UNEQ (VT-MON)

- Default Severity: Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

AUTOSW-UNEQ (VT-MON) indicates that the "UNEQ-V" alarm on page 2-233 caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (VT-MON) Alarm

Step 1 Complete the "Clear the UNEQ-V Alarm" procedure on page 2-234.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.38 AWG-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Arrayed Waveguide Gratings (AWG) Degrade alarm occurs when an DWDM card heater-control circuit degrades. The heat variance can cause slight wavelength drift. The card does not need to be replaced immediately, but it should be at the next opportunity.

Clear the AWG-DEG Alarm

Step 1 For the alarmed DWDM card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 at the next opportunity.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.39 AWG-FAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The AWG Failure alarm occurs when an DWDM card heater-control circuit completely fails. The circuit failure disables wavelength transmission. The card must be replaced to restore traffic.

Clear the AWG-FAIL Alarm

Step 1 For the alarmed DWDM card, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.40 AWG-OVERTEMP

- Default Severity: Critical (CR), Service-Affecting (SA)

- Logical Object: OTS

The AWG Over Temperature alarm is raised if a card raising an AWG-FAIL alarm is not replaced and its heater-control circuit temperature exceeds 212 degrees F (100 degrees C). The card goes into protect mode and the heater is disabled.

Clear the AWG-OVERTEMP Alarm

Step 1 Complete the "Clear the AWG-FAIL Alarm" procedure on page 2-43.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.41 AWG-WARM-UP

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The AWG Warm-Up condition occurs when a DWDM card heater-control circuit is attaining its operating temperature during startup. The condition lasts approximately 10 minutes but can vary somewhat from this period due to environmental temperature.

Note AWG-WARM-UP is an informational condition and does not require troubleshooting.

2.8.42 BAT-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Battery Fail alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so on-site information about the conditions is necessary for troubleshooting.

Clear the BAT-FAIL Alarm

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. For instructions, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.43 BKUPMEMP

- Default Severity: Critical (CR), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the TCC2 card flash memory. The alarm occurs when the TCC2 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.
- The code volume fails cyclic redundancy checking (CRC). CRC is a method to verify for errors in data transmitted to the TCC2.

The BKUPMEMP alarm can also cause the "EQPT" alarm on page 2-75. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

Caution Software updating on a standby TCC2 can take up to 30 minutes.

Clear the BKUPMEMP Alarm

Step 1 Verify that both TCC2 cards are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2 cards.

Step 2 If both cards are powered and enabled, reset the active TCC2 to make the standby TCC2 active. Complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. The ACT/STBY LED of this card should be amber and the newly active TCC2 LED should be green.

Step 3 If the TCC2 card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.44 BLSROSYNC

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The BLSR Out Of Synchronization alarm occurs during BLSR setup when you attempt to add or delete a circuit, and a working ring node loses its DCC connection because all transmit and receive fiber has been removed. CTC cannot generate the ring table and causes the BLSROSYNC alarm.

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

Clear the BLSROSYNC Alarm

Step 1 Reestablish cabling continuity to the node reporting the alarm. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for cabling information.

When the DCC is established between the node and the rest of the BLSR, it becomes visible to the BLSR and should be able to function on the circuits.

Step 2 If alarms occur when you have provisioned the DCCs, see the "2.8.76 EOC" section on page 2-72.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.45 BPV

The BPV alarm is not used in this release.

2.8.46 CARLOSS (E100T, E1000F)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: E1000F, E100T

A Carrier Loss alarm on the LAN E-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-144. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface Converter (GBIC) fiber connected to an optical card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP).

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 edge of the shelf assembly.

Clear the CARLOSS (E100T, E1000F) Alarm

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

Step 2 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to an OC-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.

Step 4 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port.

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

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

Step 6 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the Ethernet card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the Ethernet card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 8 If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps unless the Ethernet circuit is part of a manual cross-connect:

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

b. Click **Select Affected Circuits** in the shortcut menu that appears.

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

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

- Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-254 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.47 CARLOSS (EQPT)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on OC-N cards when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC2, or for the ONS 15454, the LAN backplane pin connection. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the node.

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

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

Clear the CARLOSS (EQPT) Alarm

Step 1 If the reporting card is an MXP or TXP card in an ONS 15454 node, verify the data rate configured on the pluggable port module (PPM):

a. Double-click the reporting MXP or TXP card.

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment** column and compare this with the contents of the Selected PPM area **Rate** column.

d. If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.

Step 2 If the reporting card is an OC-N card, verify connectivity by pinging the ONS 15454 that is reporting the alarm:

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

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

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

```
ping ONS-15454-IP-address
```

For example:

```
ping 198.168.10.10.
```

If the workstation has connectivity to the ONS 15454, it shows a "reply from *IP-Address*" after the ping. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 3 If the ping is successful, an active TCP/IP connection exists. Restart CTC:

a. Exit from CTC.

b. Reopen the browser.

c. Log into CTC.

Step 4 Using optical test equipment, verify that proper receive levels are achieved.

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port.

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.48 CARLOSS (FC)

The Carrier Loss alarm for Fibre Channel is not used in this release. It is reserved for future development.

2.8.49 CARLOSS (G1000)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

A Carrier Loss alarm on the LAN G-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-144. The Ethernet card has lost its link and is not receiving a valid signal.

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

- The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the

reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as the "TPTFAIL (G1000)" alarm on page 2-227 or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G1000s) alarm.

Refer to the *Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" alarm on page 2-229 for more information about alarms that occur when a point-to-point circuit exists between two cards.

Ethernet card ports must be enabled 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 edge of the shelf assembly.

Clear the CARLOSS (G1000) Alarm

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

Step 2 If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 Verify that optical receive levels are within the normal range. The correct specifications are listed in the "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71.

Step 5 If the alarm does not clear, use an Ethernet test set to determine that a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port.

Step 7 If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail:

- **a.** Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.
- **b.** Confirm that the attached Ethernet device configuration allows reception of flow control frames.

Step 8 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 9 If the alarm does not clear and the "TPTFAIL (G1000)" alarm on page 2-227 is also reported, complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-228. If the TPTFAIL alarm is not reported, continue to the next step.

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

Step 10 If the TPTFAIL alarm was not reported, determine whether a terminal (inward) loopback has been provisioned on the port:

a. In node view, click the card to go to card view.

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

c. If the service state is listed as OOS-MA, LPBK&MT, a loopback is provisioned. Go to Step 11.

Step 11 If a loopback was provisioned, complete the "Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks" procedure on page 2-255.

On the G1000-4, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 port detects the termination.

If the does not have a loopback condition, continue to Step 13.

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect:

Note An ONS 15454 Ethernet manual cross-connect is used when another vendors' equipment sits between ONS nodes, and the Open System Interconnection/Target Identifier Address Resolution Protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

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

b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.

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

d. Examine the layout of your network and determine which ONS 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

- Log into the node at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-254 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 13 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252.

Step 14 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the Ethernet card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 15 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.50 CARLOSS (GE)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: GE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on MXP and TXP card PPM clients supporting 1-Gbps or 10-Gbps traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (GE) Alarm

Step 1 Ensure that the GE client is correctly configured:

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

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment** column and compare this with the client equipment. If no PPM is provisioned, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for provisioning instructions.

d. If a PPM has been created, view the contents of the Selected PPM area **Rate** column and compare this rate with the client equipment data rate. If the PPM rate is differently provisioned, select the PPM, click **Delete**, then click **Create** and choose the correct rate for the equipment type.

Step 2 If there is no PPM misprovisioning, check for a fiber cut. An LOS alarm will also be present. If there is an alarm, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 3 If there is no fiber cut or provisioning error, check the client-side equipment for any transmission errors on the line.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.51 CARLOSS (ISC)

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Object: ISC

The Carrier Loss for Inter-Service Channel (ISC) alarm occurs on TXP card PPM clients supporting ISC client traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (ISC) Alarm

Step 1 Complete the "Clear the CARLOSS (GE) Alarm" procedure on page 2-52.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.52 CARLOSS (ML100T, ML1000, ML2)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects:ML1000, ML100T, ML2

A Carrier Loss alarm on an ML-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-144. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the Cisco IOS command line interface (CLI) as a no-shutdown port and one of the following items also occurs:

- The cable is not properly connected to the near or far port.
- Auto-negotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

For information about provisioning ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the CARLOSS (ML100T, ML1000, ML2) Alarm

Step 1 Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port.

Step 2 If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.

Step 3 If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.

Step 4 If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

Step 5 If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the Cisco IOS CLI. Autonegotiation will restart.

Step 6 If the alarm does not clear, complete the "Create the Facility (Line) Loopback on the Source-Node MXP or TXP Port" procedure on page 1-7 and test the loopback.

Step 7 If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252.

Step 8 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.53 CARLOSS (TRUNK)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

A Carrier Loss alarm on the optical trunk connecting to TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, TXPP_MR_2.5G, or MXP_2.5G_10G, MXP_2.5G_10E cards is raised when ITU-T G.709 monitoring is disabled.

Clear the CARLOSS (TRUNK) Alarm

Step 1 Complete the "Clear the LOS (2R) Alarm" procedure on page 2-139.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.54 CASETEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Case Temperature Degrade alarm is raised when a DWDM card temperature sensor detects an out-of-range external temperature at the shelf level. The working range for DWDM cards is from 23 degrees F (–5 degrees C) to 149 degrees F (65 degrees C).

Clear the CASETEMP-DEG Alarm

Step 1 Check for and resolve the "FAN" alarm on page 2-89 if it is raised against the shelf.

Step 2 If the alarm does not clear, complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-257.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.55 CKTDOWN

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: UCP-CKT

The unified control plane (UCP) Circuit Down alarm applies to logical circuits created within the UCP between devices. It occurs when there is signaling failure across a UCP interface. The failure can be caused by a number of things, such as failure to route the call within the core network. In that case, the alarm cannot be resolved from the ONS 15454 because it is an edge device.

Clear the CKTDOWN Alarm

Step 1 Ensure that the channel to neighbor has been provisioned with the correct IP address:

a. In node view, click the **Provisioning > UCP > Neighbor** tabs.

b. View the entries to find out whether the node you are trying to contact is listed.

The node name is listed under the Name column and the IP address is listed under the Node ID column. If the Node ID says 0.0.0.0 and the Enable Discovery check box is selected, the node could not automatically identify the IP address. Ping the node to ensure that it is physically and logically accessible.

c. Click **Start > Programs > Accessories > Command Prompt** to open an MS-DOS command window for pinging the neighbor.

d. At the command prompt (C:\>), type:

```
ping {node-DNS-name | node-IP-address}
```

If you typed the domain name services (DNS) name and the ping was successful, you will see:

```
pinging node-dns-name.domain-name.com. node-IP-address with 32 bytes of data:
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60

Ping statistics for IP-address:
Packets sent = 4 Received = 4 Lost = 0 (0% lost),
Approximate round trip time in milli-seconds:
Minimum = minimum-ms, Maximum = maximum-ms, Average = average-ms
```

If you typed the IP address and the ping command is successful, the result will look similar but will not include the DNS name in the first line.

e. If your DNS name or IP address ping was successful, IP access to the node is confirmed, but your neighbor configuration is wrong. Delete the neighbor by selecting it in the window and clicking **Delete**.

f. If the ping was unsuccessful, you will receive the following reply for each try:

```
Request timed out.
```

A negative reply indicates that the neighbor node is not physically or logically accessible. Resolve the access problem, which is probably a cabling issue.

Step 2 If the neighbor has not been provisioned, or if you had to delete the neighbor, create one:

a. In the Provisioning > UCP > Neighbor tabs, click the **Create** button.

b. In the Neighbor Discovery window, enter the node DNS node name in the Neighbor Name field. Leave the Enable Discovery check box checked (default setting) if you want the neighbor to be discovered through the network.

c. Click **OK**.

The node is listed in the Neighbor column list. If the neighbor discovery worked, the neighbor IP address is listed in the Node ID column. If it is not successful, the column lists 0.0.0.0.

Step 3 If neighbor discovery is enabled, ensure that the neighbor node ID and remote IP control channel (IPCC) have been discovered correctly.

Step 4 Click the **Provisioning > UCP > IPCC** tabs and view the IPCC listing. If the IPCC has been created correctly, the Remote IP column contains the neighbor IP address.

Step 5 If the neighbor IP address is not correctly discovered, the field contains 0.0.0.0.

a. Click the entry to select the neighbor IP address and click **Delete**.

b. If you get an error that will not allow you to delete the IPCC, you must delete the neighbor and recreate it. Click the **Neighbor** tab.

c. Click to select the neighbor and click **Delete**.

d. Go back to Step 2 to recreate the neighbor.

Step 6 If remote IPCC has not been discovered, or if it had to be deleted, create the connection:

a. In the Provisioning > UCP > IPCC tabs, click **Create**.

b. In the Unified Control Plane Provisioning window, click **Next**.

c. If no IPCCs are listed, click **Create**.

d. In the Create New IPCC window, click the DCC termination corresponding to the core network interface.

Leave the SDCC radio button selected (as long as DCCs have been created on the node) and leave the Leave Unchanged radio button selected.

e. Click **OK**. The IPCC is listed in the Unified Control Plane Provisioning window.

f. Click the neighbor to select it, and click **Next**.

g. Choose the UCP interface [for example, Slot 5 (OC-48), port 1] where the core network is connected from the drop-down list. The field default is the node where you are logged in.

h. Choose the UCP interface TNA address type. The default is IPv4. The address field lists the login node IP address by default.

i. Click **Finish**. If creation is successful, the Remote ID column in the IPCC tab will contain the neighbor IP address.

Step 7 Ensure that the local and remote interface IDs have been provisioned correctly:

a. Click the **Interface** tab. View the slot and port listed in the Interface column [for example, Slot 5 (OC48), port 1].

b. Compare the listed interface listed with the IPCC tab SDCC column entry.

Step 8 If the Interface column is not the same as the SDCC column entry, click the entry in the Interface window to select it and click **Delete**.

Step 9 Click **Next**.

Step 10 In the Existing CCIDs list, click the IPCC containing the DCC connection. Click **Next**.

The correct interface for the selected CCID is shown in the UPC Interface field, and the correct IP address information for the login node is shown by default in the other fields. Click **Finish**.

Step 11 If you completed all of these steps and verified the information, the alarm could be the result of a misconfiguration in the core network. Contact the core site administrators.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.56 CLDRESTART

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 power is initialized.

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 edge of the shelf assembly.

Clear the CLDRESTART Condition

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251.

Step 2 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252.

Step 3 If the condition does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.57 COMIOXC

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the XC10G cross-connect card. It occurs when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 on the reporting XC10G cross-connect card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the "Side Switch the Active and Standby XC10G Cross-Connect Cards" procedure on page 2-251.

Step 4 Complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting cross-connect card.

Step 5 If the alarm does not clear, complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-253 for the reporting cross-connect card.

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

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.58 COMM-FAIL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Plug-In Module (card) Communication Failure indicates that there is a communication failure between the TCC2 and the card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.3 CTC Card Resetting and Switching" section on page 2-249 for commonly used procedures.

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

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.59 CONTBUS-A-18

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2 slot to TCC2 slot occurs when the main processor on the TCC2 in the first slot ("TCC A") loses communication with the coprocessor on the same card. This applies to the Slot 7 TCC2.

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 edge of the shelf assembly.

Clear the CONTBUS-A-18 Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251 to make the Slot 11 TCC2 active.

Step 2 Wait approximately 10 minutes for the Slot 7 TCC2 to reset as the standby TCC2. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the Slot 11 TCC2 and complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 to return the card to the active state.

Step 4 If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.60 CONTBUS-B-18

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2 slot to TCC2 slot occurs when the main processor on the TCC2 in the second slot ("TCC B") loses communication with the coprocessor on the same card. This applies to the Slot 11 TCC2.

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 edge of the shelf assembly.

Clear the CONTBUS-B-18 Alarm

Step 1 Complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 to make the Slot 7 TCC2 active.

Step 2 Wait approximately 10 minutes for the Slot 11 TCC2 to reset as the standby TCC2. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the Slot 7 TCC2 and complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 to return the Slot 11 TCC2 card to the active state.

Step 4 If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.61 CONTBUS-IO-A

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCCA to Shelf A Slot Communication Failure alarm occurs when the active Slot 7 TCC2 (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm can appear briefly when the ONS 15454 switches to the protect TCC2. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the newly active TCC2. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2, the other card, and the backplane.

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

Clear the CONTBUS-IO-A Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-168 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 11 TCC2, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-250. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 3 If the alarm object is the standby Slot 11 TCC2, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card will remain standby.)

If CONTBUS-IO-A is raised on several cards at the same time, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1 800 553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.62 CONTBUS-IO-B

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCC B to Shelf Communication Failure alarm occurs when the active Slot 11 TCC2 (TCC B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm might appear briefly when the ONS 15454 switches to the protect TCC2. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the newly active TCC2. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2, the other card, and the backplane.

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

Clear the CONTBUS-IO-B Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-168 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 7 TCC2, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-250. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 3 If the alarm object is the standby Slot 7 TCC2, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 4 If CONTBUS-IO-A is raised on several cards at the same time, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 7 If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1 800 553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.63 CTNEQPT-MISMATCH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Connection Equipment Mismatch (CTNEQPT-MISMATCH) condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually present in the shelf. For example, an XC card may be preprovisioned in Slot 10, but an XCVT may be physically installed.

The alarm is raised against a card that is mismatched with the card. For example, CTNEQPT-MISMATCH is raised in the following situations:

- An XC card is replaced with an XCVT or XC10G card.
- An XCVT card is replaced with an XC10G card.

Note Cisco does not support configurations of unmatched cross-connect cards in Slot 8 and Slot 10, although this situation may briefly occur during the upgrade process. (For example, you might have an XC in Slot 8 and an XC10G in Slot 10 while you are upgrading Slot 10.)

Note The cross-connect card you are replacing should not be the active card. (It can be in SBY state or otherwise not in use.)

If you upgrade a node to R4.6 and replace an XC with XCVT or XC10G, or an XCVT with an XC10G, the CTNEQPT-MISMATCH condition is raised but it will be cleared when the upgrade process ends.

Note During an upgrade, this condition occurs and is raised as its default severity, Not Alarmed (NA). However, after the upgrade has occurred, if you wish to change the condition's severity so that it is Not Reported (NR), you can do this by modifying the alarm profile used at the node. For more information about modifying alarm severities, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the CTNEQPT-MISMATCH Condition

Step 1 Verify what card is preprovisioned in the slot:

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

b. View the slot's row contents in the **Eqpt Type** and **Actual Eqpt Type** columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot. For example, Slot 8 might be provisioned for an XCVT card, which is shown in the Eqpt Type column, but an XC10G card could be physically present in the slot. The XC10G would be shown in the Actual Eqpt Type column.)

Step 2 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the mismatched card.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.64 CTNEQPT-PBPROT

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the protect ONS 15454 Slot 10 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2 and the backplane.

Note This alarm automatically raises and clears when the Slot 8 XC10G cross-connect card is reseated.

Caution Software update on a standby TCC2 can take up to 30 minutes.

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 edge of the shelf assembly.

Clear the CTNEQPT-PBPROT Alarm

Step 1 If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251 for the standby TCC2 card. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the standby TCC2. Do not physically reseat an active TCC2. Doing so disrupts traffic.

Step 2 If not all cards show the alarm, perform a CTC reset on the standby XC10G card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-250. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

If the cross-connect reset is not complete and error-free or if the TCC2 reboots automatically, call Cisco TAC (1 800 553-2447).

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the standby OC-192 card.

Step 5 Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.

Step 6 If the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 on the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 10 Complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245 to switch traffic back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting traffic card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" procedure on page 2-242 for commonly used procedures.

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

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.65 CTNEQPT-PBWORK

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the ONS 15454 Slot 8 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2 and the backplane.

Note This alarm automatically raises and clears when the ONS 15454 Slot 10 XC10G cross-connect card is reseated.

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

Clear the CTNEQPT-PBWORK Alarm

Step 1 If all traffic cards show CTNEEQPT-PBWORK alarm, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 for the active TCC2 and then complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the TCC2 card. Do not physically reseat an active TCC2 card; it disrupts traffic.

Step 2 If not all traffic cards show the alarm, complete the "Side Switch the Active and Standby XC10G Cross-Connect Cards" procedure on page 2-251 for the active XC10G cross-connect card.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the standby cross-connect card.

Step 6 If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245. If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 10 If you switched traffic, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245 to switch it back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the OC-192 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 12 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting traffic card.

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.66 DATAFLT

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TCC2 exceeds its flash memory capacity.

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

Clear the DATAFLT Alarm

Step 1 Complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.67 DBOSYNC

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The standby Database Out Of Synchronization alarm occurs when the standby TCC2 "To be Active" database does not synchronize with the active database on the active TCC2.

Caution If you reset the active TCC2 card while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TCC2 database. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for instructions.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

a. In node view, click the **Provisioning > General > General** tabs.

b. In the Description field, make a small change such as adding a period to the existing entry.

The change causes a database write but does not affect the node state. The write could take up to a minute.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.68 DS3-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates a frame format mismatch on a signal transiting the ONS 15454 DS3XM-6 or DS3XM-12 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type for a DS3XM-6 card is set to C Bit and the incoming signal frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting DS3XM-6 or DS3XM-12 card.

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

Step 3 For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal (C bit or M13).

Step 4 If the Line Type field does not match the expected incoming signal, select the correct Line Type in the drop-down list.

Step 5 Click **Apply**.

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

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

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.69 DSP-COMM-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The digital signal processor (DSP) Communication Failure alarm indicates that there is a communications failure between an MXP or TXP card microprocessor and the on-board DSP chip that controls the trunk (DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP or TXP card microprocessor attempts to restore communication with the DSP chip until the alarm is cleared.

If the alarm is raised for an extended period, the MXP or TXP card raises the "DSP-FAIL" alarm on page 2-68, and could affect traffic.

Note DSP-COMM-FAIL is an informational alarm and does not require troubleshooting.

2.8.70 DSP-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The DSP Failure alarm indicates that a "DSP-COMM-FAIL" alarm on page 2-68 has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting MXP or TXP card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.71 DUP-IPADDR

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area.

Clear the DUP-IPADDR Alarm

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 In the IP Address field, change the IP address to a unique number.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.72 DUP-NODENAME

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

Step 1 In node view, click the **Provisioning > General > General** tabs.

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.73 EHIBATVG

- Default Severity: Major (MJ), Service-Affecting (NSA)
- Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.74 ELWBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.75 ENCAP-MISMATCH-P

- Default Severity: Major (MJ), Service-Affecting
- Logical Object: STS-TRM

The Encapsulation C2 Byte Mismatch Path alarm applies to ML-Series Ethernet cards. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to PLM-P, which must meet all five criteria.) For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

An example of a situation that would raise ENCAP-MISMATCH-P is if a circuit created between two ML-Series cards has generic framing procedure (GFP) framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card will transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive cards on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by a PLM-P or PLM-V.

Note By default, an ENCAP-MISMATCH-P alarm will cause an ML-Series card data link to go down. This behavior can be modified using the command line interface (CLI) command **no pos trigger defect encap**.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the ENCAP-MISMATCH-P Alarm

Step 1 Ensure that the correct framing mode is in use on the receive card:

a. In node view, double-click the receive ML-Series card to display the card view.

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

c. In the Mode drop-down list, ensure that the same mode (**GFP** or **HDLC)** is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:

a. In node view, double-click the transmit ML-Series card to display the card view.

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

c. In the Mode drop-down list, ensure that the same mode (**GFP** or **HDLC)** is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series card:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* to obtain the full configuration command sequences.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.76 EOC

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The SONET Data Communications Channel (DCC) Termination Failure alarm occurs when the ONS 15454 loses its data communications channel. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its OC-3 section overhead.

The SDCCs consist of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15454 uses the DCC on the SONET section layer to communicate network management information.

Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service (IS-NR) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

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

Note If a circuit shows a partial state when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC Alarm

Step 1 If the "LOS (DS1)" alarm on page 2-140 is also reported, complete the "Clear the LOS (DS1) Alarm" procedure on page 2-140.

Step 2 If the "SF-L" condition on page 2-208 is reported, complete the "Clear the SF-L Condition" procedure on page 2-208.

Step 3 If the alarm does not clear on the reporting node, verify the physical connections between the cards and the fiber-optic cables that are configured to carry SDCC traffic. If they are not, correct them.

If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service (IS-NR) ports. Verify that the ACT/SBY LED on each OC-N card is green.

Step 4 When the LEDs on the OC-N cards are correctly illuminated, complete the "Verify or Create Node SDCC Terminations" procedure on page 2-254 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the port is active and in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as **IS**.

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and click **IS** in the drop-down list. Click **Apply**.

Step 7 For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations.

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

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

Step 8 If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. See the "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71 for non-DWDM card levels and refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for DWDM card levels.

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

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2 switches control to the standby TCC2. If the alarm clears when the ONS 15454 node switches to the standby TCC2, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TCC2 reset does not clear the alarm, delete the problematic SDCC termination:

a. From card view, click **View > Go to Previous View** if you have not already done so.

a. Click the **Provisioning > Comm Channels > SDCC** tabs.

b. Highlight the problematic DCC termination.

c. Click **Delete**.

d. Click **Yes** in the Confirmation Dialog box.

Step 12 Recreate the SDCC termination. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for instructions.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.77 EOC-L

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Line DCC Termination Failure alarm occurs when the ONS 15454 loses its line data communications channel. For example, the OSCM card can raise this alarm on its OC-3 line overhead.

The LDCCs are nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS 15454 uses the LDCCs on the SONET line layer to communicate network management information.

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

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

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

Note If a circuit shows a partial status when the EOC alarm is raised, it occurs when the logical circuit is in place. The circuit will be able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-72.

Step 2 If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.78 EQPT

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, EQPT, PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "2.8.43 BKUPMEMP" section on page 2-45. The BKUPMEMP procedure also clears the EQPT alarm.

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited and a PROTNA alarm is raised. The standby path generates a path-type 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 edge of the shelf assembly.

Clear the EQPT Alarm

Step 1 If traffic is active on the alarmed port, you might need to switch traffic away from it. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 4 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 5 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.79 EQPT-MISS

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Replaceable Equipment or Unit Missing alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted. It might also indicate that the ribbon cable connecting the AIP to the system board is bad.

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 edge of the shelf assembly.

Clear the EQPT-MISS Alarm

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

Step 2 If the fan-tray assembly is present, complete the "Replace the Alarm Interface Panel" procedure on page 2-260.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for installation instructions.

Step 4 If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.80 ERFI-P-CONN

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication Path Connectivity condition is triggered on DS-1, DS-3, or VT circuits when the "UNEQ-P" alarm on page 2-231 and the "TIM-P" alarm on page 2-226 are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-232. This should clear the ERFI condition.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.81 ERFI-P-PAYLD

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)

- Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication Path Payload condition is triggered on DS-1, DS-3, or VT circuits when the "PLM-P" alarm on page 2-190 alarm is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

Step 1 Complete the "Clear the PLM-P Alarm" procedure on page 2-191. This should clear the ERFI condition.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.82 ERFI-P-SRVR

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication Path Server condition is triggered on DS-1, DS-3, or VT circuits when the "AIS-P" alarm on page 2-25 or the "LOP-P" alarm on page 2-136 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-137. This should clear the ERFI condition.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.83 ERROR-CONFIG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Error in Startup Configuration alarm applies to the ML-Series Ethernet cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.

Note For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the ERROR-CONFIG Alarm

Step 1 If you have a different type of ML-Series card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 2 Upload the configuration file to the TCC2:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location in the Open dialog box.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250.

Step 4 If the alarm does not clear or if your configuration file was correct according to the installed card, start a Cisco IOS CLI for the card:

a. Right click the ML-Series card graphic in node view.

b. Choose **Open IOS Connection** from the shortcut menu.

Note Open IOS Connection is not available unless the ML-Series card is physically installed in the shelf.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* to correct the errored configuration file line.

Step 5 Execute the CLI command **copy run start**. The command copies the new card configuration into the database and clears the alarm.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.84 ETH-LINKLOSS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Rear Panel Ethernet Link Removed condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Clear the ETH-LINKLOSS Condition

Step 1 To clear this alarm, reconnect the backplane LAN cable. Refer to the *Cisco ONS 15454 Procedure Guide* for instructions to install this cable.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.85 E-W-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

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

Note The E-W-MISMATCH alarm also appears during the initial set up of a ring with its East-West slots configured correctly. If the alarm appears during the initial setup, the alarm clears itself shortly after the ring setup is complete.

Note The lower-numbered slot at a node is traditionally labeled as the west slot and the higher numbered slot is labeled as the east slot. For example, Slot 6 is west and Slot 12 is east.

Note The physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slots as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

Clear the E-W-MISMATCH Alarm with a Physical Switch

Step 1 Diagram the ring setup, including nodes and spans, on a piece of paper or white board.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Label each of the nodes on the diagram with the same name that appears on the network map.

Step 4 Right-click each span to reveal the node name/slot/port for each end of the span.

Step 5 Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1—Node2/Slot6/Port1 (2F BLSR OC48, ring name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/Port 1.

Step 6 Repeat Steps 4 and 5 for each span on your diagram.

Step 7 Label the highest slot at each node east and the lowest slot at each node west.

Step 8 Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about configuring the system.

Step 9 If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.

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

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

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Clear the E-W-MISMATCH Alarm in CTC

Step 1 Log into the misconnected node. A misconnected node has both ring fibers connecting it to its neighbor nodes misconnected.

Step 2 Click the **Maintenance > BLSR** tabs.

Step 3 From the row of information for the fiber span, complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241 to identify the node ID, ring name, and the slot and port in the East Line column and West Line column. Record the above information.

Step 4 Click **View > Go to Network View**.

Step 5 Delete and recreate the BLSR:

- **a.** Click the **Provisioning > BLSR** tabs.
- **b.** Click the row from Step 3 to select it and click **Delete**.
- **c.** Click **Create**.
- **d.** Fill in the ring name and node ID from the information collected in Step 3.
- **e.** Click **Finish**.

Step 6 Display node view and click the **Maintenance > BLSR** tabs.

Step 7 Change the West Line field to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line field to the slot you recorded for the West Line in Step 3.

Step 9 Click **OK**.

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.86 EXCCOL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

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 could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2 card. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC2 for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the TCC2 card has a flow rate set to 10 Mb, half-duplex.

Step 2 If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC2 card and the network management LAN.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.87 EXERCISE-RING-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

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 is not reported.

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-134, the "LOS (OCN)" alarm on page 2-144, or BLSR alarms.

Step 2 Reissue the Exercise Ring command:

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

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

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

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.88 EXERCISE-SPAN-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISE-SPAN-FAIL 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 or ring, EXERCISE-SPAN-FAIL is not reported.

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-134, the "LOS (OCN)" alarm on page 2-144, or a BLSR alarm.

Step 2 Reissue the Exercise Span command:

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

b. Determine whether the card you would like to exercise is the west card or the east card.

c. Click the row of the affected span under the East Switch or West Switch column.

d. Select **Exercise Span** in the drop-down list.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.89 EXT

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding might have occurred.

Clear the EXT Alarm

Step 1 In node view double-click the AIC or AIC-I card to display the card view.

Step 2 Double-click the AIC or AIC-I card Maintenance > External Alarms tab.

Step 3 Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.90 EXTRA-TRAF-PREEMPT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

An Extra Traffic Preempted alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs when low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Clear the EXTRA-TRAF-PREEMPT Alarm

Step 1 Verify that the protection switch has occurred by checking the Conditions tab.

Step 2 If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm occurred on a four-fiber BLSR and the span switch occurred on this OC-N, clear the span switch on the working system.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.91 FAILTOSW

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, TRUNK

The Failure to Switch to Protection condition occurs when a working electrical card cannot switch to the protect card in a protection group because another working electrical card with a higher-priority alarm has switched to the protect card.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.

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

Step 2 If the condition does not clear, replace the working electrical card that is reporting the higher-priority alarm by following the "Physically Replace a Traffic Card" procedure on page 2-252. This card is the working electrical card using the protect card and not reporting FAILTOSW.

Replacing the working electrical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.92 FAILTOSW-PATH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection port, a lockout set on one of the path protection nodes, or path level alarms that would cause a path protection switch to fail including the "AIS-P" condition on page 2-25, the "LOP-P" alarm on page 2-136, the "SD-P" condition on page 2-206, the "SF-P" condition on page 2-209, and the "UNEQ-P" alarm on page 2-231.

The "LOF (OCN)" alarm on page 2-134, the "LOS (OCN)" alarm on page 2-144, the "SD-L" condition on page 2-205, or the "SF-L" condition on page 2-208 can also occur on the failed path.

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 edge of the shelf assembly.

Clear the FAILTOSW-PATH Alarm in a Path Protection Configuration

Step 1 Look up and clear the higher-priority alarm. Clearing this condition frees the standby card and clears the FAILTOSW-PATH condition. If the "AIS-P" condition on page 2-25, the "LOP-P" alarm on page 2-136, the "UNEQ-P" alarm on page 2-231, the "SF-P" condition on page 2-209, the "SD-P" condition on page 2-206, the "LOF (OCN)" alarm on page 2-134, the "LOS (OCN)" alarm on page 2-144, the "SD-L" condition on page 2-205, or the "SF-L" condition on page 2-208 are also occurring on the reporting port, complete the applicable alarm clearing procedure.

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

Step 2 If the alarm does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the "Physically Replace a Traffic Card" procedure on page 2-252. Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.93 FAILTOSWR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Fail to Switch to Protection Ring condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears when one of the following situations occurs:

- A physical card pull of the active TCC2 card (done under TAC supervision).
- A node power cycle.
- A higher-priority event such as an external switch command.
- The next ring switch succeeds.
- The cause of the APS switch (such as the "SD (DS1, DS3)" condition on page 2-203 or the "SF (DS1, DS3)" condition on page 2-207) 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 (IS-NR) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

Clear the FAILTOSWR Condition in a BLSR Configuration

Step 1 Perform the EXERCISE RING command on the reporting card:

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

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

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

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

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

Step 4 If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node.

Step 5 Click the **Maintenance > BLSR** tabs.

Step 6 Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards and ports and port are active and in service:

a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. Double-click the card in CTC to display the card view.

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

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

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

Step 8 If fiber continuity to the ports is okay, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the protect standby OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 13 If the condition does not clear after you replace the BLSR cards on the node one by one, repeat Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.94 FAILTOSWS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following situations occurs:

- A physical card pull of the active TCC2 done under TAC supervision.
- A node power cycle.
- A higher-priority event such as an external switch command occurs.
- The next span switch succeeds.
- The cause of the APS switch (such as the "SD (DS1, DS3)" condition on page 2-203 or the "SF (DS1, DS3)" condition on page 2-207) clears.

Clear the FAILTOSWS Condition

Step 1 Perform the EXERCISE SPAN command on the reporting card:

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

b. Determine whether the card you would like to exercise is the west card or the east card.

c. Click the row of the affected span under the East Switch or West Switch column.

d. Select **Exercise Span** in the drop-down list.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

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

Step 4 If clearing other alarms does not clear the FAILTOSWS condition, log into the near-end node.

Step 5 Click the **Maintenance > BLSR** tabs.

Step 6 Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service:

a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

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

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

Step 8 If fiber continuity to the ports is okay, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the protect standby OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 13 If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.95 FAN

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Fan Failure alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range.

The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the shelf. However, even with five working fans, the fan-tray assembly could need replacement because a sixth working fan is required for extra protection against overheating.

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

Clear the FAN Alarm

Step 1 Determine whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-257.

Step 2 If the filter is clean, complete the "Replace the Alarm Interface Panel" procedure on page 2-260.

Note The fan should run immediately when correctly inserted.

Step 3 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-259.

Step 4 If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.96 FC-NO-CREDITS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: FCMR

The Fibre Channel Distance Extension Credit Starvation alarm occurs on storage access networking (SAN) Fibre Channel/Fiber Connectivity (FICON) FC_MR-4 cards when the congestion prevents the generic framing procedure GFP transmitter from sending frames to the FC_MR-4 card port. for example, the alarm can be raised when an operator configures a card to autodetect framing credits but the card is not connected to an interoperable FC-SW-standards-based Fibre Channel/FICON port.

FC-NO-CREDITS is raised only if transmission is completely prevented. (If traffic is slowed but still passing, this alarm is not raised.) The alarm is raised in conjunction with the GFP-NO-BUFFERS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm might be raised at the upstream remote FC_MR-4 data port.

Clear the FC-NO-CREDITS Alarm

Step 1 If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode. Follow manufacturer instructions.

Step 2 If the port is not connected to a switch, turn off Autodetect Credits:

a. Double-click the FC_MR-4 card.

b. Place the port out of service (OOS,MT).

c. Click the **Provisioning > Port > Distance Extension** tabs.

d. Uncheck the **Autodetect Credits** column check box.

e. Click **Apply**.

f. Place the port back in service (IS).

Step 3 Program the Credits Available value based on the buffers available on the connected equipment:

Note The NumCredits must be provisioned to a value smaller than or equal to the receive buffers or credits available on the connected equipment.

a. Double-click the FC_MR-4 card.

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Enter a new value in the Credits Available column.

d. Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.97 FE-AIS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the "LOS (OCN)" alarm on page 2-144).

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.98 FEC-MISM

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Forward Error Correction (FEC) Mismatch alarm occurs if one end of a span using MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards is configured to use FEC and the other is not. FEC-MISM is related to ITU-T G.709 and is only raised against a trunk port.

Clear the FEC-MISM Alarm

Step 1 Double-click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G,TXP_MR_10E or TXPP_MR_2.5G card.

Step 2 Click the **Provisioning > OTN > OTN Lines** tab.

Step 3 Check the FEC column check box.

Step 4 Verify that the far-end card is configured the same way by repeating Step 1 through Step 3.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.99 FE-DS1-MULTLOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Multiple DS-1 LOS Detected condition occurs when multiple DS-1 signals are lost on a far-end DS-1 card. The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an ONS 15454 FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.100 FE-DS1-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Non-Service Affecting condition occurs when a far-end DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in an ONS 15454 Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.101 FE-DS1-SA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on a DS-1 card that affects service because traffic is unable to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.102 FE-DS1-SNGLLOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment. Signal loss also causes the "LOS (OCN)" alarm on page 2-144. The prefix FE in an alarm or condition means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SNGLLOS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SNGLLOS Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.103 FE-DS3-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-3 Equipment Failure Non-Service Affecting condition occurs when a far-end ONS 15454 DS-3 equipment failure occurs in C-bit framing mode, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-NSA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.104 FE-DS3-SA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-3 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on an ONS 15454 DS-3 card in C-bit framing mode that affects service because traffic is unable to switch to the protect port.

The prefix FE in an alarm or condition means the main alarm is occurring at the far-end node and not at the node reporting the FE condition. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-SA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.105 FE-EQPT-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: DS3

The Far End Common Equipment Failure condition occurs when a non-service-affecting equipment failure is detected on far-end DS-3 equipment. The prefix FE occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-EQPT-NSA alarm. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

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

Clear the FE-EQPT-NSA Condition

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.106 FE-FRCDWKSWBK-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

The Far End Forced Switch Back to Working—Span condition is raised on a far-end 1+1 protection port when it is Force switched to the working port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWBK-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

Clear the FE-FRCDWKSWBK-SPAN Condition

Step 1 Complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-243 for the far-end port.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.107 FE-FRCDWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs from a far-end node when a BLSR ring is forced from working to protect using the FORCE RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-RING condition does not also clear, complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.108 FE-FRCDWKSWPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the FORCE SPAN command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-FRCDWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not also clear, complete the "Clear a BLSR External Switching Command" procedure on page 2-249 for instructions.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.109 FE-IDLE

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End Idle condition occurs when a far-end node detects an idle DS-3 signal in C-bit framing mode.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-IDLE condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Clear the FE-IDLE Condition

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

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

Step 3 Clear the main alarm by clearing the protection switch. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.110 FE-LOCKOUTOFPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far-End Lock Out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a far-end node using the Lockout Protect Span command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-LOCKOUTOFPR-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOCKOUTOFPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Ensure there is no lockout set. Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.111 FE-LOF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOF condition occurs when a far-end node reports the "LOF (DS3)" alarm on page 2-133 in C-bit framing mode.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-LOF condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOF Condition

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

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

Step 3 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-133. It also applies to FE-LOF.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.112 FE-LOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOS condition occurs in C-bit framing mode when a far-end node reports the "LOS (DS3)" alarm on page 2-141.

The prefix FE occurs when the main alarm is occurring at the far-end node, and not at the node reporting the FE-LOS condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOS Condition

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

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

Step 3 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-140.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.113 FE-MANWKSWBK-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

The Far End Manual Switch Back to Working—Span condition occurs when a far-end path protection span is Manual switched back to working.

The prefix FE occurs when the main alarm is occurring at the far-end node, and not at the node reporting the FE-LOS condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWBK-SPAN Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.114 FE-MANWKSWPR-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when a BLSR working ring is switched from working to protect at a far-end node using the MANUAL RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-MANWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.115 FE-MANWKSWPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber BLSR span is switched from working to protect at the far-end node using the Manual to Protect command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

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

Step 3 Complete the "Clear a BLSR External Switching Command" alarm on page 2-249.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.116 FEPRLF

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Protection Line Failure alarm occurs when an APS channel "SF (DS1, DS3)" condition on page 2-207 occurs on the protect card coming into the node.

Note The FEPRLF only alarm occurs when bidirectional protection is used on optical cards in a 1+1 configuration or four-fiber BLSR configuration.

Clear the FEPRLF Alarm on a Four-Fiber BLSR

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

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for instructions.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.117 FIBERTEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Fiber Temperature Degrade alarm occurs when a DWDM card internal heater-control circuit fails. Degraded temperature can cause some signal drift. The card should be replaced at the next opportunity.

Clear the FIBERTEMP-DEG Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 at the next opportunity.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.118 FORCED-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Force Switch Request condition occurs when you enter the Force command on a port or span to force traffic from a working port or working span to a protection port or protection span (or vice versa). You do not need to clear the condition if you want the Force switch to remain.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition is raised against a card, complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-243.

Step 3 If it is raised against a span, complete the "Clear Path Protection Span External Switching Command" procedure on page 2-247.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.119 FORCED-REQ-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Force Switch Request Ring condition applies to optical trunk cards when the FORCE RING command is applied to two-fiber and four-fiber BLSRs to move traffic from working to protect.

Clear the FORCED-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.120 FORCED-REQ-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, OCN, TRUNK

The Force Switch Request Span condition applies to optical trunk cards in two-fiber or four-fiber BLSRs when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.121 FRCDSWTOINT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.

Note FRCDSWTOINT is an informational condition and does not require troubleshooting.

2.8.122 FRCDSWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.

Note FRCDSWTOPRI is an informational condition and does not require troubleshooting.

2.8.123 FRCDSWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.

Note FRCDSWTOSEC is an informational condition and does not require troubleshooting.

2.8.124 FRCDSWTOTHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to the third timing source.

Note FRCDSWTOTHIRD is an informational condition and does not require troubleshooting.

2.8.125 FRNGSYNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

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 node has lost its designated building integrated timing supply (BITS) timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 node relying on an internal clock.

Note If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Alarm

Step 1 If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about timing.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-223 and the "SYNCSEC" alarm on page 2-223.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.126 FSTSYNC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

A Fast Start Synchronization mode alarm occurs when the node is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note FSTSYNC is an informational alarm. It does not require troubleshooting.

2.8.127 FULLPASSTHR-BI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic and there is a change in the receive K byte from No Request.

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.128 GAIN-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Gain High Degrade alarm is raised on OPT-BST and OPT-PRE amplifier cards when the gain reaches the high degrade threshold and is prevented from reaching the setpoint due to an internal failure. The card should be replaced at the first opportunity.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HDEG Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level in CTC:

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

b. Display the optical thresholds by clicking the OPT-BST or OPT-PRE **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab.

Step 4 If the power value is outside the expected range, verify that all impacted optical signal sources are in IS-NR service state and that their outputs are within expected range. Optical signal sources include the trunk port of a TXP or MXP card, or an ITU-T line card.

Step 5 If the signal source is OOS,DSBLD admin state, put it in IS state. This will create the IS-NR service state.

Step 6 If the service state is IS-NR but the output power is outside of specifications, complete the "Clear the LOS-P (OCH, OMS, OTS) Alarm" procedure on page 2-150.

Step 7 If the signal source is IS and the power is within the expected range, go back to the unit reporting the alarm and clean the fiber connected to amplifier's COM-RX port according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note Unplugging fiber from the COM-RX port can cause a traffic hit. To avoid this, perform a traffic switch if possible using the procedures outlined in the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more in-depth information about protection switches, refer to the *Cisco ONS 15454 Reference Manual.*

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem. To do this, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for acceptance testing procedures that can be used for troubleshooting purposes.

Step 9 If no other alarms exist that could be the source of the GAIN-HDEG, or if clearing an alarm did not clear the GAIN-HDEG, place all of the card ports in OOS,DSBLD admin state.

Step 10 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.129 GAIN-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Gain High Fail alarm is raised on OPT-BST and OPT-PRE amplifier cards when the gain crosses the high failure point threshold. The card will need to be replaced.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HFAIL Alarm

Step 1 For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-105.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.130 GAIN-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Gain Low Degrade alarm is raised on OPT-BST and OPT-PRE amplifier cards when the gain has crossed the low degrade threshold and is prevented from reaching the setpoint due to an internal failure. The card should be replaced at the first opportunity.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LDEG Alarm

Step 1 For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-105.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.131 GAIN-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Gain Low Fail alarm is raised on OPT-BST and OPT-PRE amplifier cards when the gain crosses the low failure point threshold. The card will need to be replaced.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LFAIL Alarm

Step 1 For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-105.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.132 GCC-EOC

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The GCC Embedded Operation Channel Failure alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The GCC-EOC is raised when the channel cannot operate.

Clear the GCC-EOC Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-72.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.133 GE-OOSYNC

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: FC, GE, ISC, TRUNK

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G cards when the Gigabit Ethernet signal is out of synchronization and is very similar to the SONET LOS alarm. This alarm can occur when you try to input a SONET signal to the TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card. A signal is present, so there is no CARLOSS alarm, but it is not correctly formatted for the card and so it raises the GE-OOSYNC alarm.

Clear the GE-OOSYNC Alarm

Step 1 Ensure that the incoming signal is provisioned with the correct physical-layer protocol.

Step 2 Ensure that the line is provisioned with the correct line speed (10 Gbps).

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.134 GFP-CSF

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T, ML2

The GFP Client Signal Fail Detected alarm is a secondary alarm raised on local GFP data ports when a remote service-affecting alarm causes invalid data transmission. The alarm is raised locally on FC_MR-4, ML100T, ML1000, MXP_MR_25G, MXPP_MR_25G GFP data ports and does not indicate that a service-affecting failure is occurring at the local site, but that a CARLOSS, LOS, or SYNCLOSS alarm is affecting a remote data port's transmission capability.

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the GFP-CSF Alarm

Step 1 Clear the service-affecting alarm at the remote data port.

Step 2 If the GFP-CSF alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.135 GFP-DE-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T

The GFP Fibre Channel Distance Extension Mismatch alarm indicates that a port configured for Distance Extension is connected to a port that is not operating in Cisco's proprietary Distance Extension mode. It is raised on Fibre Channel and FICON card GFP ports supporting distance extension. The alarm occurs when distance extension is enabled on one side of the transport but not on the other. To clear, distance extension must be enabled on both ports connected by a circuit.

Clear the GFP-DE-MISMATCH Alarm

Step 1 Ensure that the data extension protocol is configured correctly on both sides:

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

b. Place the port in the OOS,MT state.

c. Click the **Provisioning > Port > Distance Extension** tabs.

d. Check the check box in the **Enable Distance Extension** column.

e. Click **Apply**.

f. Place the port back IS-NR admin state

Step 2 If the GFP-DE-MISMATCH alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.136 GFP-EX-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/FICON cards when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds.

The user needs to make sure that both end ports are sending a null extension header for a GFP frame. The FC_MR-4 card always sends a null extension header, so if the equipment is connected to other equipment vendors, those need to be provisioned appropriately.

Clear the GFP-EX-MISMATCH Alarm

Step 1 Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)

Step 2 If the GFP-EX-MISMATCH alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.137 GFP-LFD

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T, ML2

The GFP Loss of Frame Delineation alarm applies to Fibre Channel/FICON GFP ports and occurs if there is a bad SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. The loss causes traffic stoppage.

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the GFP-LFD Alarm

Step 1 Look for and clear any associated SONET path errors such as LOS or AIS-L originating at the transmit node.

Step 2 If the GFP-LFD alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.138 GFP-NO-BUFFERS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T

The GFP Fibre Channel Distance Extension Buffer Starvation alarm is raised on Fibre Channel/FICON card ports supporting GFP and the distance extension protocol when the GFP transmitter cannot send GFP frames due to lack of remote GFP receiver buffers. This occurs when the remote GFP-T receiver experiences congestion and is unable to send frames over the Fibre Channel/FICON link.

This alarm might be raised in conjunction with the FC-NO-CREDITS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm might be raised at the upstream remote FC_MR-4 data port.

Clear the GFP-NO-BUFFERS Alarm

Step 1 Complete the "Clear the FC-NO-CREDITS Alarm" procedure on page 2-90.

Step 2 If the GFP-CSF alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.139 GFP-UP-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: GFP-FAC, ML1000, ML100T

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel 1 Gig or Fibre Channel 2 Gig and the remote port media type could be set to FICON 1 Gig or FICON 2 Gig.

Clear the GFP-UP-MISMATCH Alarm

Step 1 Ensure that the transmit port and receive port are provisioned the same way for distance extension:

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

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Check the check box in the **Enable Distance Extension** column.

d. Click **Apply**.

Step 2 Ensure that both ports are set for the correct media type. For each port, complete the following:

a. Double-click the card to display the card view (if you are not already in card view).

b. Click the **Provisioning > Port> General** tabs.

c. Choose the correct media type (Fibre Channel 1 Gbps, Fibre Channel 2 Gbps, FICON 1 Gbps, or FICON 2 Gbps) from the drop-down list.

d. Click **Apply**.

Step 3 If the GFP-UP-MISMATCH alarm does not also clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.140 HELLO

- Default Severity: Minor (MN), Non-Service-Affecting (NSA)
- Logical ObjectS: EC1-12, OCN

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or an OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

Step 1 Ensure that the area ID is correct on the missing neighbor:

a. In node view, click the **Provisioning > Network > OSPF** tabs.

b. Ensure that the IP address in the Area ID column matches the other nodes.

c. If the address does not match, click the incorrect cell and correct it.

d. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.141 HIBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

Clear the HIBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.142 HI-CCVOLT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: BITS

The 64K Composite Clock High NE Voltage alarm occurs when the 64K signal peak voltage exceeds 1.1 v.

Clear the HI-CCVOLT Condition

Step 1 Lower the source voltage to the clock.

Step 2 If the condition does not clear, add more cable length or add a 5 dB attenuator to the cable.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.143 HI-LASERBIAS

- Default Severity: Minor (MN), Non-Service Affecting (NSA)

- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Clear the LASEREOL Alarm" procedure on page 2-126. Replacement is not urgent and can be scheduled during a maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.144 HI-LASERTEMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN, PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength. (Two degrees Celsius is equivalent to about 200 picometers in the wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The "LOS (OCN)" alarm on page 2-144 is raised at the far-end node and the "DSP-FAIL" alarm on page 2-68 is raised at the near end. To verify the card laser temperature level, double-click the card in node view and click the Performance > Optics PM tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Clear the HI-LASERTEMP Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting MXP or TXP card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.145 HI-RXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Step 1 Find out whether gain (the amplification power) of any amplifiers has been changed. This change also causes channel power to need adjustment.

Step 2 Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.

Note If the card is part of an amplified DWDM system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

Step 4 If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at the same time and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dB.

Step 5 If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance, according to standard practice.

Step 6 If the alarm does not clear and no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71 and test the loopback.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-252. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.146 HITEMP

- Default Severity: Critical (CR), Service-Affecting (SA) for NE
- Default Severity: Minor (MN), Non-Service Affecting (NSA) for EQPT
- Logical Objects: EQPT, NE

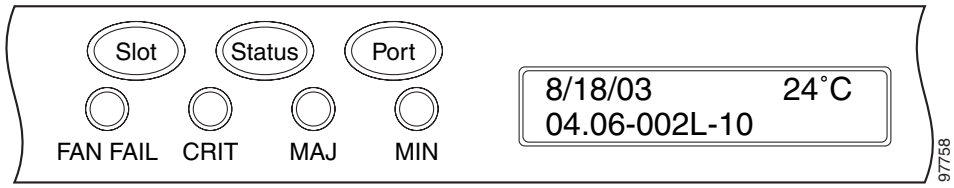
The High Temperature alarm occurs when the temperature of the ONS 15454 is above 122 degrees F (50 degrees C).

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

Clear the HITEMP Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-2).

Figure 2-2 Shelf LCD Panel



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

Step 3 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 shelf.

Step 4 If airflow is not blocked, physically ensure that blank faceplates fill the ONS shelf empty slots. Blank faceplates help airflow.

Step 5 If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-257.

Step 6 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-259.

Note The fan should run immediately when correctly inserted.

Step 7 If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447) if it applies to the NE, or a non-service-affecting problem if it applies to equipment.

2.8.147 HI-TXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Clear the HI-TXPOWER Alarm

Step 1 In node view, display the card view for the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card.

Step 2 Click the **Provisioning > Optical Thresholds** tabs.

Step 3 Decrease (change toward the negative direction) the TX Power High column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.148 HLDOVRSYNC

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: NE-SREF

The Holdover Synchronization Mode alarm indicates a loss of the primary or secondary timing reference. Timing reference loss occurs when line coding on the timing input is different from the configuration on the ONS 15454. It also usually occurs during the selection of a new node reference

clock. The HLDOVRSYNC alarm indicates that the ONS 15454 has gone into holdover and is using the ONS node internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

Clear the HLDOVRSYNC Alarm

Step 1 Clear additional alarms that relate to timing, such as:

- FRNGSYNC, page 2-103
- FSTSYNC, page 2-104
- HLDOVRSYNC, page 2-116
- LOF (BITS), page 2-131
- LOS (BITS), page 2-139
- MANSWTOINT, page 2-165
- MANSWTOPRI, page 2-165
- MANSWTOSEC, page 2-165
- MANSWTOTHIRD, page 2-165
- SWTOPRI, page 2-221
- SWTOSEC, page 2-221
- SWTOTHIRD, page 2-221
- SYNC-FREQ, page 2-222
- SYNCPRI, page 2-223
- SYNCSEC, page 2-223
- SYNCTHIRD, page 2-224

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

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.149 I-HITEMP

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15454 is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Step 1 Complete the "Clear the HITEMP Alarm" procedure on page 2-115.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447) in order to report a service-affecting problem.

2.8.150 IMPROPRMVL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: EQPT, PPM

The Improper Removal equipment alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node. It can also occur if the card is inserted into a slot but is not fully plugged into the backplane. For PPMs, the alarm occurs if you provision a PPM but no physical module is inserted on the port.

Caution Do not remove a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot. When you delete the card, CTC will lose connection with the node view and go to network view.

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 edge of the shelf assembly.

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

Note It can take up to 30 minutes for software to be updated on a standby TCC2 card.

Clear the IMPROPRMVL Alarm

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

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

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

Step 3 If any ports on the card are in service, place them out of service (OOS,MT):

Caution Before placing a port out of service (OOS,MT or OOS,DSBLD), ensure that no live traffic is present.

a. In node view, double-click the reporting card to display the card view.
b. Click the **Provisioning > Line** tab.
c. Click the **Admin State** column of any in-service (IS) ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-254.

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

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

a. Click **View > Go to Previous View** to return to node view.
b. If you are already in node view, click the **Provisioning > Protection** tabs.
c. Click the protection group of the reporting card.
d. Click **Delete**.

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

a. Click the ONS 15454 **Provisioning > Comm Channels > SDCC** tabs.
b. Click the slots and ports listed in DCC terminations.
c. Click **Delete** and click **Yes** in the dialog box that appears.

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

a. Click the **Provisioning > Timing** tabs.
b. Under NE Reference, click the drop-down arrow for **Ref-1**.
c. Change Ref-1 from the listed OC-N card to **Internal Clock**.
d. Click **Apply**.

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

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.151 INC-ISD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OOS-MA,MT service state. It is resolved when the OOS-MA,MT state ends.

Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.8.152 INHSWPR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a 1:N protection scheme, traffic can be switched between working cards when the switch to protect is disabled.

Clear the INHSWPR Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-243.

Step 2 If it is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245 to switch it back.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.153 INHSWWKG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a protection scheme, traffic can be switched between protect cards when the switch to working is disabled.

Clear the INHSWWKG Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-243.

Step 2 If it is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245 to switch traffic back.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.154 INTRUSION-PSWD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a settable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a settable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if lockout is permanent.

Clear the INTRUSION-PSWD Condition

Step 1 In node view, click the **Provisioning > Security** tabs.

Step 2 Click the **Clear security intrusion alarm** button.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.155 INVMACADR

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AIP

The Equipment Failure Invalid MAC Address alarm occurs when the ONS 15454 Media Access Control layer address (MAC Address) is invalid. Each ONS 15454 has a unique, permanently assigned MAC address. The address resides on an AIP EEPROM. The TCC2 card reads the address value from the AIP chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

Under normal circumstances, the read-only MAC address can be viewed in the Provisioning/Network tab in CTC.

The ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you will see a PARTIAL circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit end-to-end information.

An invalid MAC address can by caused when:

- There is a read error from the AIP during bootup; in this case, the reading TCC2 uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2 cards that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad.

Clear the INVMACADR Alarm

Step 1 Check for any outstanding alarms that were raised against the active and standby TCC2 and resolve them.

Step 2 If the alarm does not clear, determine whether the LCD display on the fan tray (Figure 2-2 on page 2-115) is blank or if the text is garbled. If so, proceed to Step 8. If not, continue with Step 3.

Step 3 At the earliest maintenance window, reset the standby TCC2:

Note The reset will take approximately five minutes. Do not perform any other step until the reset is complete.

a. Log into a node on the network. If you are already logged in, continue with Step b.

b. Identify the active TCC2 card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

c. Right-click the standby TCC2 card in CTC.

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

e. Click **Yes** in the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

f. Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

g. Double-click the node and ensure that the reset TCC2 card is still in standby mode and that the other TCC2 card is active.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

h. Ensure that no new alarms appear in the Alarms window in CTC that are associated with this reset.

If the standby TCC2 fails to boot into standby mode and reloads continuously, the AIP is probably defective. In this case, the standby TCC2 is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2 reloads until it reads the EEPROM. Proceed to Step 8.

Step 4 If the standby TCC2 rebooted successfully into standby mode, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251.

Resetting the active TCC2 causes the standby TCC2 to become active. The standby TCC2 keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

Step 5 After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

Step 6 Complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 again to place the standby TCC2 back into active mode.

After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2 resets, this indicates that the AIP is probably defective. Proceed to Step 8.

If the INVMACADR was raised during one TCC2 reset and cleared during the other, the TCC2 that was active while the alarm was raised needs to be replaced. Continue with Step 7.

Step 7 If the faulty TCC2 is currently in standby mode, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for this card. If the faulty TCC2 card is currently active, during the next available maintenance window complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250 and then complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Note If the replacement TCC2 is loaded with a different software version from the current TCC2 card, the card bootup might take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2 version software is copied to the new standby card.

Step 8 Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node's previous MAC address.

Step 9 Replace the ribbon cable between the system board and the AIP with a known-good cable.

Step 10 If the alarm persists, complete the "Replace the Alarm Interface Panel" procedure on page 2-260.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.156 IOSCFGCOPY

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The IOS Configuration Copy in Progress condition occurs on ML-Series Ethernet cards when a Cisco IOS startup configuration file is being uploaded or downloaded to or from an ML-Series card. (This condition is very similar to the "SFTWDOWN" condition on page 2-209 but it applies to ML-Series Ethernet cards rather than to the TCC2.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the "NO-CONFIG" condition on page 2-173 might be raised.)

Note IOSCFGCOPY is an informational condition.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.157 KB-PASSTHR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The K Bytes Pass Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are not active and the node is in K Byte pass-through state. It also occurs when a BLSR ring is being exercised using the Exercise Ring command.

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.158 KBYTE-APS-CHANNEL-FAILURE

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Channel Failure alarm is raised when a span is provisioned for different APS channels on each side. For instance, the alarm is raised if K3 is selected on one end and F1, E2, or Z2 is selected on the other end.

This alarm is also raised during checksum failure if the K1 and K2 bytes are overwritten by test equipment. It is not raised in bidirectional full pass-through or K-byte pass-through states. The alarm is overridden by AIS-P, LOF, LOS, or SF-BER alarms.

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

Step 1 The alarm is most frequently raised due to mismatched span provisioning. In this case, reprovision one side of the span with the same parameters. To do this, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2 card. In this case, complete the "Side Switch the Active and Standby XC10G Cross-Connect Cards" procedure on page 2-251 to allow CTC to resolve the issue.

Step 3 If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.159 LAN-POL-REV

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Lan Connection Polarity Reversed condition is not raised in shelves that contain TCC2 cards. It is raised by the TCC+ card during software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The TCC+ automatically compensates for this reversal, but LAN-POL-REV stays active.

Clear the LAN-POL-REV Condition

Step 1 Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.160 LASER-APR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Automatic Power Reduction (APR) alarm condition is raised by OSC-CSM, OSCM, OPT-BST, and OPT-PRE cards when the laser is working in power reduction mode. The condition clears as soon as safety conditions are released and the power value reaches the normal setpoint.

Note LASER-APR is an informational condition and does not require troubleshooting.

2.8.161 LASERBIAS-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Laser Bias Current Degrade alarm occurs on amplifier cards such as the OPT-BST or OPT-PRE when laser aging causes a degrade, but not failure, of laser transmission. The card should be replaced at the next opportunity.

Clear the LASERBIAS-DEG Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 at the next opportunity.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.162 LASERBIAS-FAIL

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Bias Current Failure alarm occurs on amplifier cards such as OPT-BST or OPT-PRE when the laser control circuit fails or if the laser itself fails service. The card must be replaced to restore traffic.

Clear the LASERBIAS-FAIL Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.163 LASEREOL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Laser Approaching End of Life alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It is typically accompanied by the "HI-LASERBIAS" alarm on page 2-112. It is an indicator that the laser in the card will need to be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, the card must be replaced sooner.

Clear the LASEREOL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.164 LASERTEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Temperature Degrade alarm occurs when the Peltier control circuit fails on an amplifier card such as the OPT-BST or OPT-PRE. The Peltier control provides cooling for the amplifier. The card should be replaced at the next opportunity.

Clear the LASERTEMP-DEG Alarm

Step 1 For the alarmed optical amplifier card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 at the next opportunity.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.165 LCAS-CRC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-Series Ethernet cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

The condition can occur if an LCAS-enabled node (containing ML2 cards) transmitting to another LCAS-enabled node delivers faulty traffic due to an equipment or SONET path failure. Transmission errors would also be reflected in CV-P, ES-P, or SES-P performance monitoring statistics. If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition will not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition will persist on the VCG.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LCAS-CRC Condition

Step 1 Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.

Step 2 Look for and clear any bit error rate alarms such as SDBER or SFBER at the transmit node.

Step 3 If no equipment or SONET path errors exist, ensure that the remote node has LCAS enabled on the circuit:

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

b. Choose the VCAT circuit and click **Edit**.

c. In the Edit Circuit window, click the **General** tab.

d. Verify that the Mode column says **LCAS**.

Step 4 If the column does not say LCAS, complete the "Delete a Circuit" procedure on page 2-254 and recreate it in LCAS mode using the instructions in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.166 LCAS-RX-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Fail condition is raised against FC_MR-4 cards and ML-Series Ethernet cards with LCAS-enabled VCG or software-enabled LCAS (SW-LCAS) VCG.

Note ML1-series and FC_MR-4 cards, used in the ONS 15454, are SW-LCAS enabled.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SONET path failure (a unidirectional failure as seen by the receive side).
- VCAT member is set out of group at the transmit side, but is set in group at the receive side.
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side.

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SONET path failure.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LCAS-RX-FAIL Condition

Step 1 Check for and clear any line or path alarms.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.167 LCAS-TX-ADD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-Series Ethernet cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed.

Note LCAS-TX-ADD is an informational condition and does not require troubleshooting.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.168 LCAS-TX-DNU

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Do Not Use (DNU) State condition is raised on FC_MR-4 cards and ML-Series Ethernet cards when the transmit side of an LCAS VCG member is in the DNU state. For a unidirectional failure, this condition is only raised at the source node.

The node reporting this condition will likely report an RDI-P alarm, and the remote node will likely report a path alarm such as AIS-P or UNEQ-P.

Note LCAS-TX-DNU is an informational condition and does not require troubleshooting.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.169 LKOUTPR-S

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Lockout of Protection Span condition occurs when path protection traffic is locked out of a protect span using the Lockout of Protect command.

Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.170 LMP-HELLODOWN

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UPC-IPCC

The Link Management Protocol (LMP) Hello Down alarm occurs when the Hello protocol, which monitors UCP control channel status, is not available for link management. The unavailability can be caused by physical layer errors (such as cabling) or by control channel misconfiguration.

Clear the LMP-HELLODOWN Alarm

Step 1 Verify that the transmit and receive cables are not crossed at each end (login site and neighbor site).

Step 2 Verify that the "LOF (OCN)" alarm on page 2-134 is not present on the source or destination nodes. If so, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 3 If the alarm does not clear, complete the "Clear the CKTDOWN Alarm" procedure on page 2-55 to verify that IPCC provisioning is valid on both ends of the user-to-network interface (UNI).

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.171 LMP-NDFAIL

- Default Severity: Minor (MN) Non-Service Affecting (NSA)
- Logical Object: UCP-IPCC

The LMP Neighbor Detection Fail alarm occurs when neighbor detection within the UCP has failed. LMP-NDFAIL can be caused by physical failure (such as cabling) between the neighbors or by control channel misconfiguration.

Clear the LMP-NDFAIL Alarm

Step 1 Complete the "Clear the LMP-HELLODOWN Alarm" procedure on page 2-130.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.172 LOA

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.

Note This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

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

Step 2 Click the alarmed VCG and then click **Edit**.

Step 3 In the Edit Circuit dialog box, click **Show Detailed Map** to see the source and destination circuit slots, ports, and STSs.

Step 4 Identify whether the STS travels across different fibers. If it does, complete the "Delete a Circuit" procedure on page 2-254.

Step 5 Recreate the circuit using the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.173 LOCKOUT-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N card or a lockout switch request on a path protection at the path level. A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear Path Protection Span External Switching Command" procedure on page 2-247.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.174 LOF (BITS)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on theTCC2 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.

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 edge of the shelf assembly.

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

Clear the LOF (BITS) Alarm

Step 1 Verify that the line framing and line coding match between the BITS input and the TCC2:

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

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

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

d. Verify that Coding matches the coding of the BITS timing source, either B8ZS or AMI.

e. If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.

f. Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

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

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the TCC2.

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

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.175 LOF (DS1)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream. If the LOF appears on theDS1N-14 card, the transmitting equipment could have its framing set to a format that differs from the receiving node.

Clear the LOF (DS1) Alarm

Step 1 Verify that the line framing and line coding match between the DS1N-14 port and the signal source:

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

b. Find the coding and framing formats of the signal source for the card reporting the alarm. You might need to contact your network administrator for the format information.

c. Display the card view of the reporting ONS 15454 card.

d. Click the ONS 15454 **Provisioning > Line** tabs.

e. Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.

g. Click **Apply**.

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

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

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.176 LOF (DS3)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment could be set to a format that differs from the receiving system. On DS3XM-6 cards, the alarm occurs only on cards with the provisionable framing format set to C bit or M13 and not on cards with the provisionable framing format is set to unframed.

Clear the LOF (DS3) Alarm

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

a. Display the card view of the reporting card.

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

c. Verify that the line type of the reporting port matches the line type of the signal source.

d. If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the drop-down list.

e. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.177 LOF (EC1-12)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EC1-12

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

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

Clear the LOF (EC1-12) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the alarm does not clear, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2 to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.178 LOF (OCN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The LOF alarm occurs when a port on the reporting card has an LOF condition. It can also occur on ONS 15454 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G,TXP_MR_10E, or TXPP_MR_2.5G cards reporting LOF. The alarm 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.

When the alarm is raised on an OC-N card, it is sometimes an indication that the OC-N card 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 edge of the shelf assembly.

Clear the LOF (OCN) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the alarm does not clear, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2 to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.179 LOF (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Frame for the DWDM trunk applies to the trunk optical or electrical signal that is carried to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It indicates that the receiving ONS 15454 has lost frame delineation in the incoming data from trunk that serves the cards. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (TRUNK) Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-135.

Step 2 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.180 LO-LASERTEMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)

- Logical Objects: EC1-12, OCN

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (Two degrees Celsius is equivalent to about 200 picometers in the wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The "LOS (OCN)" alarm on page 2-144 is raised at the far-end node and the "DSP-FAIL" alarm on page 2-68 is raised at the near end. To verify the card laser temperature level, double-click the card in node view and click the Performance > Optics PM > Current PM tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Clear the LO-LASERTEMP Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting MXP or TXP card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.181 LOM

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSTRM, TRUNK, VT-TERM

The Optical Transport Unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than three milliseconds.

Clear the LOM Alarm

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-205.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.182 LOP-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

For FC_MR-4 card, an LOP-P will be raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

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 edge of the shelf assembly.

Clear the LOP-P Alarm

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this will cause the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.

Step 4 If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-254.

Step 5 Recreate the circuit for the correct size. For instructions, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.183 LOP-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

The LOP VT alarm indicates a loss of pointer at the VT level.

The LOP-V alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

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

Clear the LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-137.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.184 LO-RXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.

Note If the card is part of an amplified DWDM system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

Step 4 If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

Step 5 If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error readings you get will not be as precise, but you will generally know whether the fiber is faulty.

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

Step 7 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the "Create the Facility (Line) Loopback on the Source-Node MXP or TXP Port" procedure on page 1-7 and test the loopback.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-252. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 9 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.185 LOS (2R)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object:

The Loss of Signal for a 2R Client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Clear the LOS (2R) Alarm

Step 1 Complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.186 LOS (BITS)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2 has an LOS from the BITS timing source. The LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.

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

Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.187 LOS (DS1)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A LOS (DS1) alarm for a DS-1 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line.

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

Clear the LOS (DS1) Alarm

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

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is not currently assigned, place the port out of service using the following steps:

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

b. For a DS1 card, click the **Maintenance > Loopback** tabs. For a DS-1 line on a DS3XM-6 or DS3XM-12 card, click the **Maintenance > DS1** tabs.

c. Under Admin State, click **OOS,DSBLD**.

d. Click **Apply**.

Step 4 If the port is assigned, verify that the correct port is in service:

a. To confirm this physically, confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine this virtually, double-click the card in CTC to display the card view:

- Click the **Provisioning > Line** tabs.
- Verify that the Admin State column lists the port as **IS**.
- If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 7 If there is a valid signal, replace the electrical connector on the ONS 15454.

Step 8 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port.

Step 9 Repeat Steps 1 to 8 for any other port on the card that reports the LOS.

Step 10 If no other alarms are present that could be the source of the LOS (DS-1), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.188 LOS (DS3)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The LOS (DS3) for a DS-3 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

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

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (DS3) Alarm

Step 1 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-140.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.189 LOS (EC1-12)

- Default Severity: Critical (CR), Service-Affecting (SA)

- Logical Object: EC1-12

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

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

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (EC1-12) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the LED is correctly lit on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

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

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 4 If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 5 If a valid signal exists, replace the cable connector on the ONS 15454.

Step 6 Repeat Steps 1 through 5 for any other port on the card that reports the LOS (EC1-12).

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 8 If no other alarms exist that could be the source of the LOS (EC1-12), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.190 LOS (ESCON)

The LOS alarm for the ESCON Object is not used in this platform in this release. It is reserved for future development.

2.8.191 LOS (FUDC)

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a UDC circuit created on an AIC-I UDC port but the port is not receiving signal input. The downstream node will have an AIS condition raised against the AIC-I port transmitting the UDC. FUDC refers to the 64-kb user data channel using the F1 byte.

Clear the LOS (FUDC) Alarm

Step 1 Verify cable continuity to the AIC-I UDC port.

Step 2 Verify that there is a valid input signal using a test set.

Step 3 If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 4 If the alarm does not clear, verify that the UDC is provisioned:

a. At the network view, click the **Provisioning > Overhead Circuits** tabs.

b. If no UDC circuit exists, create one. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

c. If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.

Step 5 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 6 If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.192 LOS (ISC)

- Default Severity: Major (MJ), Service Affecting (SA)
- Logical Object: ISC

The LOS alarm for the ISC port applies to TXP_MR_2.5G client PPMs provisioned at the ISC port rate. Troubleshooting is similar to the LOS (2R) alarm.

Clear the LOS (ISC) Alarm

Step 1 Complete the "Clear the LOS (2R) Alarm" procedure on page 2-139.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.193 LOS (MSUDC)

The LOS (MSUDC) alarm is not used in this platform in this release. It is reserved for future development.

2.8.194 LOS (OCN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

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

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

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

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

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (OCN) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the LED is correctly illuminated on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as **IS**.

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card receiver specifications. The "1.9.3 OC-N Card Transmit and Receive Levels" section on page 1-71 lists these specifications for each OC-N card. For DWDM card levels, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 7 Repeat Steps 1 to 6 for any other port on the card reporting the LOS (OC-N).

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.195 LOS (OTS)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The Loss of Signal for the OTS applies to the LINE-3-RX port of the OPT-BST amplifier and the LINE-2-RX port of the OSC-CSM card. It indicates that a fiber cut has occurred and no power is being received from the span. The alarm is raised when both LOS-P and LOS-O alarms occur, and demotes them.

Clear the LOS (OTS) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin value of the Line 4-1-RX port) is within the expected range shown in Cisco MetroPlanner. To check the level:

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

b. Click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.

c. Compare the opwrMin (dBm) column value with the MetroPlanner-generated value. (For more information about using MetroPlanner, refer to the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5*.

Step 4 If the optical power level is within specifications, check and modify the channel LOS and OSC LOS thresholds, then run automatic node setup (ANS) to execute the changes:

a. In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

b. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to decide what values to use, then modify the following items:

- West Side Rx. Channel OSC LOS Threshold
- West Side Rx. Channel LOS Threshold

c. Click the **WDM-ANS > Port Status** tabs.

d. Click **Launch ANS** and click **Yes** in the confirmation dialog box.

Step 5 If the optical power is outside of the expected range, check the power level transmitted at the other side of the span using CTC:

a. On the transmitting node, double-click the transmitting MXP or TXP to display the card view.

b. Click the **Provisioning > Optics Thresholds** tab.

c. View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.

Step 6 If the transmitted power value is within the expected range, clean the receiving node (where the LOS is raised) and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 7 If the transmitted power value is outside of the expected range, troubleshoot using the DWDM acceptance tests in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.196 LOS (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Signal for a TRUNK applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Clear the LOS (TRUNK) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, verify that the correct port is in service:

a. Confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as **IS**.

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the TXP or MXP card receiver specifications. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for levels.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

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

Step 7 Repeat Steps 1 to 6 for any other port on the card reporting the LOS (TRUNK).

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.197 LOS-O

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: OCH, OMS, OTS

The Incoming Overhead Loss of Signal alarm applies to the OSC-RX port of OPT-BST (LINE-2-RX), the OSC-RX port of OSCM (LINE-1-RX), and the internal optical port of OSC-CSM card (LINE-3-RX Port 3). It is raised when the monitored input power crosses the FAIL-LOW threshold and the OSC signal is lost. The is alarm is demoted if another LOS alarm is also present.

Clear the LOS-O Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level:

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

b. Display the optical thresholds by clicking the following tabs:

- OPT-BST **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- OSCM **Provisioning > Optical Line > Optics Thresholds** tab

Step 4 If the optical power level is within specifications, check and modify the OSC LOS threshold, then run ANS to execute the changes:

a. In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

b. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to decide upon values, then modify the West Side Rx. Channel OSC LOS Threshold.

c. Click the **WDM-ANS > Port Status** tabs.

d. Click **Launch ANS** and click **Yes** in the confirmation dialog box.

Step 5 If the port power is outside of the expected range, verify that OSC connections have been created on the other side of the span. If the connections are not present, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures.

Step 6 If OSC connections are present, check the OSC transmitted power using CTC:

a. On the transmitting node, double-click the transmitting OSC-CSM to display the card view.

b. Click the **Provisioning > Optics Thresholds** tab.

c. View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.

Step 7 If the transmitted OSC value is out of range, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for DWDM acceptance test procedures that will aid in troubleshooting the problem.

Step 8 If the OSC value is within range, come back to the port reporting the LOS-O alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 9 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 10 If no other alarms exist that could be the source of the LOS-O, or if clearing an alarm did not clear the LOS-O, place all of the card ports in OOS,DSBLD admin state.

Step 11 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external traffic switch if possible.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.198 LOS-P (OCH, OMS, OTS)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: OCH, OMS, OTS

The Path Loss of Signal Absent alarm applies to all input ports of AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32WSS, and OSC-CSM cards. It indicates that there is a loss or received signal at the OSC-CSM card or the OPT-BST card Line-1-TX (COM-TX) port and that the monitored input power has crossed the opwrMin threshold.

Clear the LOS-P (OCH, OMS, OTS) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level:

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

b. Display the optical thresholds by clicking the following tabs:

- OPT-BST **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- OPT-PRE **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- AD-xC **Provisioning > Optical Chn> Optics Thresholds** tab
- AD-xB **Provisioning > Optical Band > Optics Thresholds** tab
- 32DMX **Provisioning > Optical Chn > Optics Thresholds** tab
- 32MUX **Provisioning > Optical Chn > Optics Thresholds** tab
- 32WSS **Provisioning > Optical Chn: Optical Connector** *x* **> Optics Thresholds** tab
- OSCM **Provisioning > Optical Line > Optics Thresholds** tab.

Step 4 If the optical power level is within specifications, check the opwrMin threshold. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to decide upon values, then modify the value as necessary.

Step 5 If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS admin state by clicking the appropriate tab:

- MXPP_MR_2.5G **Provisioning > Line > OC48** tab

- MXP_2.5G_10E **Provisioning > Line > Trunk** tab
- MXP_2.5G_10G **Provisioning > Line > SONET** tab
- MXP_MR_2.5G **Provisioning > Line > OC48** tab
- TXPP_MR_2.5G **Provisioning > Line > OC48** tab
- TXP_MR_10E **Provisioning > Line > SONET** tab
- TXP_MR_10G **Provisioning > Line > SONET** tab
- TXP_MR_2.5G **Provisioning > Line > SONET** tab

If it is not IS, choose **IS** from the admin state drop-down list.

If the alarm does not clear, continue by completing the "Clear the LOS-P (TRUNK) Alarm" procedure on page 2-152.

Step 6 If the signal source is IS-NR and within the expected range, come back to the port reporting the LOS-P alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for basic instructions, or to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more detailed information.

Step 7 Repeat Steps 1 through 6 for any other port on the card reporting the LOS-P alarm.

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS-P, or if clearing an alarm did not clear the LOS-P, place all of the card ports in OOS,DSBLD admin state.

Step 10 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.199 LOS-P (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Path Loss of Signal Absent alarm applies to all input ports of AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32WSS, and OSC-CSM cards when there is a loss or received signal at an input port caused by MXP or TXP transmit port errors.

Clear the LOS-P (TRUNK) Alarm

Step 1 On the transmit MXP or TXP card, check the output power using CTC:

a. On the transmitting node, double-click the card to display the card view.

b. Click the **Provisioning > Optics Thresholds** tab.

c. View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.

Step 2 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 3 If no other alarms exist that could be the source of the LOS-P, or if clearing an alarm did not clear the LOS-P, place all of the card ports in OOS,DSBLD admin state.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.200 LO-TXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-TXPOWER Alarm

Step 1 Display the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card view.

Step 2 Click the **Provisioning > Optical Thresholds** tabs.

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 5 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.201 LPBKCRS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an OC-192 card. A cross-connect loopback test occurs below line speed and does not affect traffic.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the optical card in CTC to display the card view.

Step 2 Complete the "Clear an OC-N Card XC Loopback Circuit" procedure on page 2-255.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.202 LPBKDS1FEAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Caused by Far-End Alarm and Control (FEAC) Command DS-1 condition on DS3XM-6 and DS3XM-12 cards occurs when a DS-1 loopback signal is received from the far-end node due to a FEAC command. An FEAC command is often used with loopbacks.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKDS1FEAC Condition

Step 1 In node view, double-click the DS3XM-6 or DS3XM-12 card to display the card view.

Step 2 Click the **Maintenance > DS1** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.203 LPBKDS1FEAC-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The DS-1 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-1 FEAC loopback.

Note LPBKDS1FEAC-CMD is an informational condition and does not require troubleshooting.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

2.8.204 LPBKDS3FEAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6, DS3XM-12, DS3-12E, or DS3/EC1-48 card loopback signal is received in C-bit framing mode from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by these DS cards. DS3XM-6, DS3XM-12, and DS3/EC1-48 cards generate and report FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

Note LPBKDS3FEAC is an informational condition and does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

Step 1 In node view, double-click the DS-3 card to display the card view.

Step 2 Click the **Maintenance > DS3** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.205 LPBKDS3FEAC-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-3 FEAC loopback.

Note LPBKDS3FEAC-CMD is an informational condition and does not require troubleshooting.

2.8.206 LPBKFACILITY (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Loopback Facility condition on MXP and TXP card client port indicates that there is an active facility (line) loopback on the port. For this condition to be present, the admin state is OOS,MT and the service state is OOS-MA, LPBK & MT.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (TRUNK) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.207 LPBKFACILITY(DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Facility condition occurs when a software facility (line) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6 or DS3XM-12 card.

Note CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

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

Clear the LPBKFACILITY (DS1, DS3) Condition

Step 1 Complete the "Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.208 LPBKFACILITY (EC1-12)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EC1-12

A Loopback Facility condition occurs when a software facility (line) loopback is active for a port on the reporting EC1-12 card.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (EC1-12) Condition

Step 1 Complete the "Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.209 LPBKFACILITY (ESCON)

The Loopback Facility condition for ESCON is not used in this platform in this release. It is reserved for future development.

2.8.210 LPBKFACILITY (FC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FC

A Loopback Facility condition occurs on an FC when a software facility (line) loopback is active for an MXPP_MR_2.5G or TXPP_MR_2.5G card client PPM provisioned at the FC1G or FC2G line speed.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKFACILITY (FC) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.211 LPBKFACILITY (FCMR)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

A Loopback Facility for FCMR condition occurs when a facility loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKFACILITY (FCMR) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.212 LPBKFACILITY (G1000)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A Loopback Facility condition occurs when a software facility (line) loopback is active for a port on the reporting G-Series Ethernet card.

Facility loopbacks are described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (G1000) Condition

Step 1 Complete the "Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.213 LPBKFACILITY (GE)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: GE

A Loopback Facility condition for a GE port occurs when a software facility (line) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, or TXPP_MR_2.5G card client PPM provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM provisioned at the TEN_GE port rate.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKFACILITY (GE) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.214 LPBKFACILITY (ISC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: ISC

A Loopback Facility condition for an ISC port occurs when a software facility (line) loopback is active for a TXP_MR_2.5G client PPM provisioned at the ISC port rate.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKFACILITY (ISC) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.215 LPBKFACILITY (ML2)

The Facility Loopback condition for an ML2 card is not used in this platform in this release and is reserved for future development. The ML2 object is currently used only in the ONS 15310 platform.

2.8.216 LPBKFACILITY (OCN)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

A Loopback Facility condition occurs when a software facility (line) loopback is active for a port on the reporting OC-N card.

Facility loopbacks are described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

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

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (OCN) Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-254.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

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

2.8.217 LPBKTERMINAL (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Loopback Terminal condition on MXP or TXP client or trunk cards indicates that there is an active terminal (inward) loopback on the port.

Clear the LPBKTERMINAL (TRUNK) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.218 LPBKTERMINAL (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6 or DS3XM-12 card. DS-1 and DS-3 terminal loopbacks do not typically return an AIS signal.

Facility loopbacks are described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (DS1, DS3) Condition

Step 1 Complete the "Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.219 LPBKTERMINAL (EC1-12)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EC1-12

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting EC1-12 card.

For information about troubleshooting optical circuits, refer to the"1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (EC1-12) Condition

Step 1 Complete the "Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.220 LPBKTERMINAL (ESCON)

The Loopback Terminal condition for ESCON is not used in this platform in this release. It is reserved for future development.

2.8.221 LPBKTERMINAL (FC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FC

A Loopback Terminal condition occurs on an FC when a software terminal (inward) loopback is active for an MXPP_MR_2.5G or TXP_MR_2.5G card client PPM provisioned at the FC1G or FC2G line speed.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (FC) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.222 LPBKTERMINAL (FCMR)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

A Loopback Terminal for FCMR condition occurs when a terminal loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (FCMR) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.223 LPBKTERMINAL (G1000)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting G-Series Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-4 card, the outgoing signal is not transmitted; it is only redirected in the receive direction.

For more information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (G1000) Condition

Step 1 Complete the "Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks" procedure on page 2-255.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.224 LPBKTERMINAL (GE)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: GE

A Loopback Terminal condition for a GE port occurs when a software terminal (inward) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, or TXPP_MR_2.5G card client PPM provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM provisioned at the TEN_GE port rate.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (GE) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.225 LPBKTERMINAL (ISC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: ISC

A Loopback Terminal condition for an ISC port occurs when a software terminal (inward) loopback is active for a TXP_MR_2.5G client PPM provisioned at the ISC port rate.

For information about troubleshooting optical circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (ISC) Condition

Step 1 Complete the "Clear an MXP, TXP, or FCMR Card Loopback Circuit" procedure on page 2-256.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.226 LPBKTERMINAL (ML2)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: ML2

The Terminal Loopback condition for the ML2 card is not currently used in the ONS 15454 platform and is reserved for future development. The ML object is currently used only in the ONS 15310 platform.

2.8.227 LPBKTERMINAL (OCN)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting card. OC-N terminal loopbacks do not typically return an AIS.

Note Performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For information about troubleshooting circuits, refer to the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (OCN) Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-254.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.228 LWBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

Clear the LWBATVG Alarm

Step 1 The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.229 MAN-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N card or BLSR path. Clearing the Manual switch clears the MAN-REQ condition.

Clear the MAN-REQ Condition

Step 1 If the condition is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-245. If it is raised against a BLSR path, complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.230 MANRESET

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

Note MANRESET is an informational condition and does not require troubleshooting.

2.8.231 MANSWTOINT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to the internal timing source.

Note MANSWTOINT is an informational condition and does not require troubleshooting.

2.8.232 MANSWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

Note MANSWTOPRI is an informational condition and does not require troubleshooting.

2.8.233 MANSWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to the second timing source.

Note MANSWTOSEC is an informational condition and does not require troubleshooting.

2.8.234 MANSWTOTHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the tertiary timing source.

Note MANSWTOTHIRD is an informational condition and does not require troubleshooting.

2.8.235 MANUAL-REQ-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on two-fiber and four-fiber BLSR rings to switch from working to protect or protect to working.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.236 MANUAL-REQ-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Manual Switch Request on Ring condition occurs on BLSRs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span.

Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-249.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.237 MEA (AIP)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

Clear the MEA (AIP) Alarm

Step 1 Complete the "Replace the Alarm Interface Panel" procedure on page 2-260.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.238 MEA (BIC)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: BIC

The Missing Equipment Attributes alarm for the backplane interface connector (BIC) indicates a compatibility issue in using high-density DS-3 cards with universal backplane interface connectors (UBIC) and an older shelf backplane. Backplane versions 15454-HA-SD and later are compatible with the UBIC with horizontal connectors (UBIC-H) and UBIC with vertical connectors (UBIC-V) that the high-density EC-1, DS-1, and DS-3 electrical connections require. The MEA alarm is raised if you attempt to install a high-density card into Slots 4, 5, 6, 12, 13, or 14 with an older noncompatible backplane installed. The card is not usable in this case. It is also raised if you attempt to use an older BIC with the newer backplane.

Clear the MEA (BIC) Alarm

Step 1 Click the **Provisioning > Inventory** tabs to determine your backplane model. If the backplane is not a 15454-HA-SD, replace the backplane or do not attempt to use high-density DS-3 cards. Table 2-10 lists the BICs that are compatible with various backplanes.

Table 2-10 BIC Compatibility Matrix

BIC Type	Part No.
BICs that work with the current and previous backplane	MANUF_EQPT_ID_BIC_A_SMB_HD_BP
	MANUF_EQPT_ID_BIC_B_SMB_HD_BP
	MANUF_EQPT_ID_BIC_A_BNC_24_HD_BP
	MANUF_EQPT_ID_BIC_A_BNC_48_HD_BP
	MANUF_EQPT_ID_BIC_B_SMB
	MANUF_EQPT_ID_BIC_B_SMB_ALT
	MANUF_EQPT_ID_BIC_B_BNC_24
	MANUF_EQPT_ID_BIC_B_BNC_48

Table 2-10 BIC Compatibility Matrix (continued)

BIC Type	Part No.
New HD BICs that work only with the new backplanes	MANUF_EQPT_ID_BIC_A_UNIV_VERT
	MANUF_EQPT_ID_BIC_B_UNIV_VERT
	MANUF_EQPT_ID_BIC_A_UNIV_HORIZ
	MANUF_EQPT_ID_BIC_B_UNIV_HORIZ
	MANUF_EQPT_ID_BIC_A_MINI_BNC_HD_BP
	MANUF_EQPT_ID_BIC_B_MINI_BNC_HD_BP
High-density BICs that work only with 15454-HA-SD	MANUF_EQPT_ID_BIC_A_SMB
	MANUF_EQPT_ID_BIC_A_SMB_ALT
	MANUF_EQPT_ID_BIC_A_BNC_24
	MANUF_EQPT_ID_BIC_A_BNC_48

Step 2 If you determine that your BIC type and backplane are compatible despite the MEA alarm, or if the alarm does not clear after you resolve the incompatibilities, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.239 MEA (EQPT)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly.

Removing the incompatible cards clears the alarm.

Note If an OC3-8 card is installed in Slots 5 to 6 and 12 to 13, it does not appear in CTC and raises an MEA.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that sits in the slot reporting the MEA alarm. In node view, click the **Inventory** tab.

Step 2 Determine whether the ONS 15454 shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed above, then you are using an earlier shelf assembly.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 3 Verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card faceplate.

- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 4.
- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed. Proceed to the Step 4.

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

- If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to Step 4.
- If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the 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 Proceed to Step 4.

Step 4 If you prefer the card type depicted by CTC, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

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

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

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

Step 6 If any ports on the card are in service, place them out of service (OOS,MT):

Caution Before placing ports out of service, ensure that live traffic is not present.

a. Double-click the reporting card to display the card view.
b. Click the **Provisioning** tab.
c. Click the admin state of any in-service ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 7 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-254.

Caution Before deleting the circuit, ensure that live traffic is not present.

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

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

Step 9 Right-click the card reporting the alarm.

Step 10 Choose **Delete**.

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

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.240 MEA (FAN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

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

Clear the MEA (FAN) Alarm

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

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.

Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.

Step 2 If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 2-259.

Step 3 If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the "Replace the Fan-Tray Assembly" procedure on page 2-259.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.241 MEA (PPM)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: PPM

The Missing Equipment Attributes alarm for the pluggable port module (PPM) is raised on DWDM cards when the PPM is misprovisioned or unsupported. It can occur when you plug in a PPM without first preprovisioning it, or when you provision the PPM for a wavelength that is explicitly not the first tunable wavelength.

Clear the MEA (PPM) Alarm

Step 1 To provision the PPM you must first create it in CTC. To do this, complete the following steps:

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

b. Click the **Provisioning > Pluggable Port Modules** tabs. (If you already see the PPM listed in the Pluggable Port Modules Area, go to Step 2.)

c. Under the Pluggable Port Modules area, click **Create**.

d. In the Create PPM dialog box, choose the PPM number from the drop-down list (for example, PPM 1).

e. Choose the PPM type from the second drop-down list, for example PPM (1 Port).

f. Click **OK**.

Step 2 After you have created the PPM, or if you see it listed in the Pluggable Port Modules area but not in the Selected PPM area, choose the port rate:

a. Under the Selected PPM area, click **Create**.

b. In the Create Port dialog box, choose the port (for example, 1-1) from the drop-down list.

c. Choose the correct port type from the drop-down list. (For more information about selecting PPM port types, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

d. Click **OK**.

Step 3 If you see the port listed in the Pluggable Port Modules area and the Selected PPM, the MEA indicates that the incorrect port rate was selected. Click the port in the Selected PPM area and click **Delete**.

Step 4 Complete Step 2 to correctly provision the port rate.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.242 MEM-GONE

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2 card. CTC does not function properly until the alarm clears. The alarm clears when additional memory becomes available.

Note The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.243 MEM-LOW

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2 card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC2 is exceeded, CTC ceases to function.

Note The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.244 MFGMEM

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2 card cannot read this memory. EEPROM stores manufacturing data that a system TCC2 uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause minor problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon will be grayed out in CTC network view.

Tip When you lose LAN connectivity with an ONS 15454 due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2 LAN port.

Clear the MFGMEM Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 2 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Step 3 If the MFGMEM alarm continues to report after replacing the TCC2s, the problem is with the EEPROM.

Step 4 If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 2-259.

Step 5 If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.245 NO-CONFIG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The No Startup Configuration condition applies to ML-Series Ethernet cards and occurs when no startup configuration file has been downloaded to the TCC2, whether or not you preprovision the card slot. This alarm is to be expected during provisioning. When the startup configuration file is copied to the active TCC2, the alarm clears.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the NO-CONFIG Condition

Step 1 Create a startup configuration for the card in Cisco IOS.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 2 Upload the configuration file to the TCC2:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.246 OCHNC-INC

The OCHNC-INC condition is not used in this platform n this release. It is reserved for future development.

2.8.247 ODUK-1-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-1-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-1-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

ODUK-x-AIS-PM can occur singly when one far-end client signal is lost or it can occur multiply (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-1-AIS-PM Condition

Step 1 Look for and clear the LOS (2R) alarm on far-end client. This should clear the ODUK-1-AIS-PM condition on trunk.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.248 ODUK-2-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-2-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-2-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

ODUK-x-AIS-PM can occur singly when one far-end client signal is lost or it can occur multiply (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-2-AIS-PM Condition

Step 1 Complete the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-174.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.249 ODUK-3-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-3-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-3-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

ODUK-x-AIS-PM can occur singly when one far-end client signal is lost or it can occur multiply (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-3-AIS-PM Condition

Step 1 Complete the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-174.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.250 ODUK-4-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-4-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-4-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

ODUK-x-AIS-PM can occur singly when one far-end client signal is lost or it can occur multiply (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-4-AIS-PM Condition

Step 1 Complete the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-174.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.251 ODUK-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the "LOS (OCN)" alarm on page 2-144 occurring downstream. The ODUK-AIS-PM condition is reported in the path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by the upstream "ODUK-OCI-PM" condition on page 2-177.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-AIS-PM Condition

Step 1 Determine whether upstream nodes and equipment have alarms, especially the "LOS (OCN)" alarm on page 2-144, or OOS ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.252 ODUK-BDI-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP cards or MXP cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-BDI-PM Condition

Step 1 Complete the "Clear the OTUK-BDI Condition" procedure on page 2-184.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.253 ODUK-LCK-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-LCK-PM Condition

Step 1 Unlock the upstream node signal.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.254 ODUK-OCI-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes an "ODUK-LCK-PM" condition on page 2-177 downstream.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-OCI-PM Condition

Step 1 Verify the fiber connectivity at nodes upstream.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.255 ODUK-SD-PM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line bit error rate (BER) has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-SD-PM Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-205.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.256 ODUK-SF-PM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-SF-PM Condition

Step 1 Complete the "Clear the SF (DS1, DS3) Condition" procedure on page 2-208.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.257 ODUK-TIM-PM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Trace Identifier Mismatch (TIM) PM condition applies to the path monitoring area of the OTN overhead for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes a "ODUK-BDI-PM" condition on page 2-176 downstream.

The ODUK-TIM-PM condition applies to TX cards and MXP cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the ODUK-TIM-PM Condition

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-227.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.258 OOU-TPT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused. It occurs in conjunction with the "VCG-DEG" alarm on page 2-235.

Clear the OOT-TPT Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-235. Clearing that condition clears this condition as well.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.259 OPTNTWMIS

- Default Severity: Major (MJ), Non-Service Affecting (NSA)

- Logical Object: NE

The Optical Network Type Mismatch alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore or MetroAccess. All DWDM nodes on the same network must be configured for the same network type because APC and automatic node setup (ANS) behave differently on each of these network types.

When the OPTNTWMIS occurs, the "APC-DISABLED" alarm on page 2-27 could also be raised.

Clear the OPTNTWMIS Alarm

Step 1 In node view of the alarmed node, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Choose the correct option from the Network Type list box, and click **Apply**.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.260 OPWR-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power High Degrade alarm occurs on all DWDM ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports, and the OSC-CSM and OSCM OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the high degrade threshold. For 32DMX, 32DMX-O, 32MUX-O, and 32WSS OCH ports and OSC-CSM and OSCM OSC-TX ports, OPWR-HDEG indicates that the card has a variable optical attenuator (VOA) control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-HDEG Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the power read by photodiode on the port is within the expected range foreseen by MetroPlanner. The application generates a spreadsheet of values containing this information.

Step 4 If the optical power level is within specifications, check the opwrMin threshold. Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* and decide what value to use for modifying the value:

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

b. Display the optical thresholds by clicking the following tabs:

- OPT-BST **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab
- OPT-PRE **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab

- AD-xC **Provisioning > Optical Chn> Optics Thresholds** tab
- AD-xB **Provisioning > Optical Band > Optics Thresholds** tab
- 32DMX **Provisioning > Optical Chn > Optics Thresholds** tab
- 32MUX **Provisioning > Optical Chn > Optics Thresholds** tab
- 32WSS **Provisioning > Optical Chn: Optical Connector** *x* **> Optics Thresholds** tab
- OSCM **Provisioning > Optical Line > Optics Thresholds** tab

Step 5 If the received optical power level is within specifications, consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to determine the correct levels and check the opwrMin threshold. If necessary, modify the value as required.

Step 6 If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS admin state by clicking the correct tab:

- MXPP_MR_2.5G **Provisioning > Line > OC48** tab
- MXP_2.5G_10E **Provisioning > Line > Trunk** tab
- MXP_2.5G_10G **Provisioning > Line > SONET** tab
- MXP_MR_2.5G **Provisioning > Line > OC48** tab
- TXPP_MR_2.5G **Provisioning > Line > OC48** tab
- TXP_MR_10E **Provisioning > Line > SONET** tab
- TXP_MR_10G **Provisioning > Line > SONET** tab
- TXP_MR_2.5G **Provisioning > Line > SONET** tab

If it is not IS-NR, choose **IS** from the admin state drop-down list. This will create the IS-NR service state.

Step 7 If the port is in IS-NR service state but its output power is outside of the specifications, complete the "Clear the LOS-P (OCH, OMS, OTS) Alarm" procedure on page 2-150.

Step 8 If the signal source is IS and within expected range, come back to the unit reporting OPWR-HDEG and clean all connected fiber in the same line direction as the reported alarm according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242. For more detailed protection switching information, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide.*

Step 9 Repeat Steps 1 to 8 for any other port on the card reporting the OPWR-HDEG alarm.

Step 10 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 11 If no other alarms exist that could be the source of the OPWR-HDEG, or if clearing an alarm did not clear the alarm, place all of the card ports in OOS,DSBLD admin state.

Step 12 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.261 OPWR-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm occurs on an OPT-BST or OPT-PRE amplifier card AOTS port if the transmitted power exceeds the high fail threshold. This alarm is raised only in control power working mode. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-HFAIL Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-180.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.262 OPWR-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Low Degrade alarm occurs on all ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports; and the OSC-CSM and OSCM card OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the low degrade threshold. For the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports and the OSC-CSM and OSCM card OSC-TX ports, OPWR-HDEG indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-LDEG Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-180.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.263 OPWR-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm applies to OPT-BS T and OPT-PRE amplifier AOTS ports. It also applies to AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32DMX, 32WSS, and OSC-CSM transmit (TX) ports. The alarm is raised when monitored input power crosses the low fail threshold.

For the AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x card OCH ports and the 32MUX-O, 32DMX, 32DMX-O; 32WSS, OSCM, and OSC-CSM cards, OPWR-LFAIL indicates that the card has a VOA control circuit failure that affects its attenuation capability.

Clear the OPWR-LFAIL Alarm

Step 1 Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-180.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.264 OSRION

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Optical Safety Remote Interlock On condition is raised for OPT-PRE and OPT-BST amplifier cards when OSRI is set to ON. The condition does not correlate with the "OPWR-LFAIL" alarm on page 2-183 also reported on the same port.

Clear the OSRION Condition

Step 1 Turn the OSRI off:

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

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

c. In the OSRI column, choose **OFF** from the drop-down list.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.265 OTUK-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition, such as the "LOS (OCN)" alarm on page 2-144, is occurring downstream. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.266 OTUK-BDI

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK BDI condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-BDI is indicated by the BDI bit in the section monitoring overhead. The alarm occurs when there is an SF condition upstream. OTUK-BDI is triggered by the "OTUK-TIM" condition on page 2-186.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-BDI Condition

Step 1 Determine whether upstream nodes have the "OTUK-AIS" condition on page 2-183.

Step 2 In the upstream node, click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card in node view to display the card view.

Step 3 Click the **Provisioning > OTN > Trail Trace Identifier** tabs.

Step 4 Compare the Current Transmit String with the Current Expected String in the downstream node. (Verify the Current Expected String by making the same navigations in another CTC session to the downstream node.)

Step 5 If the two do not match, modify the Current Expected String.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.267 OTUK-IAE

The OTUK-IAE alarm is not used in this platform in this release. It is reserved for future development.

2.8.268 OTUK-LOF

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The OTUK-LOF alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card of MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-LOF Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-135.

Step 2 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.269 OTUK-SD

- Default Severity: Not Alarmed (NA) Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SD condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-SD Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-205.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.270 OTUK-SF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SF condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-SF Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-205.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.271 OTUK-TIM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-TIM alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled and section trace mode is set to manual. The alarm indicates that the expected TT1 string does not match the received TTI string in the optical transport unit overhead of the digital wrapper. OTUK-TIM triggers an "ODUK-BDI-PM" condition on page 2-176.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-TIM Condition

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-227.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.272 OUT-OF-SYNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: FC, GE, ISC, TRUNK

The Ethernet Out of Synchronization condition occurs on TXP_MR_2.5 and TXPP_MR_2.5 cards when the PPM port is not correctly configured for the Gigabit Ethernet payload rate.

Clear the OUT-OF-SYNC Condition

Step 1 Double-click the alarmed card to display the card view.

Step 2 Delete the provisioning for the PPM:

a. Click the PPM in the Selected PPM area.

b. Click **Delete**.

Step 3 Recreate the PPM provisioning using the correct data rate:

a. Click **Create**.

b. In the Port Type drop-down list, choose **ONE_GE**.

c. Click **OK.**

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.273 PARAM-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Plug-in Module Range Settings Mismatch condition is raised for OPT-BST and OPT-PRE amplifier cards, optical add-drop multiplexer (OADM) cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x), multiplexer cards (32MUX-O and 32WSS), and demultiplexer cards (32DMX-O and 32DMX) when the parameter range values stored on the card are different from the parameters stored in TCC2 database. The condition is not user-serviceable. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.274 PDI-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15454 STS path overhead. The alarm indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The "AIS" condition on page 2-24 often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P will clear the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the "TPTFAIL (G1000)" alarm on page 2-227 or the "CARLOSS (G1000)" alarm on page 2-49 reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the "TPTFAIL (ML1000, ML100T, ML2)" alarm on page 2-228 reported against one or both packet-over-SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for more information about ML-Series cards.

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

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

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

Clear the PDI-P Condition

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

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists the circuit as active.

c. If the Status column lists the circuit as PARTIAL, wait 10 minutes for the ONS 15454 to initialize fully. If the PARTIAL status does not change after full initialization, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

Step 2 After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

Step 3 If traffic is affected, complete the "Delete a Circuit" procedure on page 2-254.

Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for detailed procedures to create circuits.

Step 5 If circuit deletion and recreation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 8 If the condition does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the optical/electrical cards.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 9 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.275 PEER-NORESPONSE

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

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

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.276 PLM-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition occurs due to a problematic C2 byte value in the SONET path overhead. The alarm is raised if all of the following conditions are met:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped, unspecified).
- The received C2 byte is not 0x01 (equipped, unspecified).

For example, on nodes equipped with CTC Software R4.1 and earlier, this alarm could occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

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

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

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

Clear the PLM-P Alarm

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-188.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.277 PLM-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: VT-TERM

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15454s interoperate with equipment that performs bit-synchronous mapping for DS-1. The ONS 15454 uses asynchronous mapping.

Clear the PLM-V Alarm

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

Step 2 If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.278 PORT-ADD-PWR-DEG-HI

The Add Port Power High Degrade alarm is not used in this platform in this release. It is reserved for future development.

2.8.279 PORT-ADD-PWR-DEG-LOW

The Add Port Power Low Degrade alarm is not used in this platform in this release. It is reserved for future development.

2.8.280 PORT-ADD-PWR-FAIL-HI

The Add Port Power High Fail alarm is not used in this platform in this release. It is reserved for future development.

2.8.281 PORT-ADD-PWR-FAIL-LOW

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCH

The Add Port Power Low Fail alarm occurs on a 32WSS ADD port if an internal signal transmission crosses the low fail threshold and prevents the signal output power from reaching its setpoint. This alarm indicates that the card has a VOA control circuit failure, which affects the card automatic signal attenuation. The alarmed card should be replaced at the next opportunity.

Clear the PORT-ADD-PWR-FAIL-LOW Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level:

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

b. Display the optical thresholds by clicking the 32WSS **Provisioning > Optical Chn: Optical Connector** *x* **> Optics Thresholds** tab.

Step 4 If the optical power level is within specifications, check the opwrMin threshold and consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* to determine the correct value. Modify the value as necessary.

Step 5 If the power value is outside the expected range verify that the trunk port of a TXP, MXP or ITU-T line card connected to ADD-RX port is in IS-NR service state by clicking the correct tab:

- MXPP_MR_2.5G **Provisioning > Line > OC48** tab
- MXP_2.5G_10E **Provisioning > Line > Trunk** tab
- MXP_2.5G_10G **Provisioning > Line > SONET** tab
- MXP_MR_2.5G **Provisioning > Line > OC48** tab
- TXPP_MR_2.5G **Provisioning > Line > OC48** tab
- TXP_MR_10E **Provisioning > Line > SONET** tab
- TXP_MR_10G **Provisioning > Line > SONET** tab
- TXP_MR_2.5G **Provisioning > Line > SONET** tab

If it is not IS-NR, choose **IS** from the admin state drop-down list. This will create the IS-NR service state.

Step 6 If the port is in IS-NR service state but its output power is outside of the specifications, complete the "Clear the LOS-P (OCH, OMS, OTS) Alarm" procedure on page 2-150.

Step 7 If the signal source is IS-NR and within expected range, come back to the port reporting the PORT-ADD-PWR-FAIL-LOW alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 8 Repeat Steps 1 through 7 for any other port on the card reporting the alarm.

Step 9 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 10 If no other alarms exist that could be the source of the PORT-ADD-PWR-FAIL-LOW, or if this procedure did not clear the alarm, place all of the card ports in OOS,DSBLD admin state.

Step 11 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for short-version procedures. For more detailed protection switching information, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.282 PORT-MISMATCH

- Default Severity: Critical (CR), Service-Affecting ()
- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA) for FCMR
- Logical Objects: 2R, ESCON, FC, FCMR, GE, ISC

The Pluggable Port Mismatch alarm applies to ML-Series Ethernet card SFP connectors. The alarm indicates that the provisioned payload for the connector does not match the SFP configuration.

The error must be resolved in the Cisco IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.283 PRC-DUPID

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

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.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241.

Step 3 Repeat Step 2 for all the nodes on the ring.

Step 4 If two nodes have an identical node ID number, complete the "Change a BLSR Node ID Number" procedure on page 2-241 so that each node ID is unique.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.284 PROTNA

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC2 or XC10G cross-connect card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant TCC2 card installed and provisioned in the chassis.

Step 2 If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):

a. In CTC, double-click the reporting card to display the card view (if the card is not an XC10G cross-connect card).

b. Click the **Provisioning** tab.

c. Click the admin state of any in-service (IS) ports.

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

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.285 PTIM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The Payload Type Identifier Mismatch alarm occurs when there is a mismatch between the way the ITU-T G.709 option is configured on MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card at each end of the optical span.

Clear the PTIM Alarm

Step 1 Double-click the alarmed MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card to display the card view.

Step 2 Click the **Provisioning > OTN > OTN Lines** tabs.

Step 3 Ensure that the G.709 OTN check box is checked. If not, check it and click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.286 PWR-FAIL-A

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), XC card, OC-N cards, or TCC2 card.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.**

Clear the PWR-FAIL-A Alarm

Step 1 If a single card has reported the alarm, take the following actions depending on the reporting card:

- If the reporting card is an active traffic line port in a 1+1 or part of a path protection, ensure that an automatic protection switch (APS) traffic switch has occurred to move traffic to the protect port.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

Step 2 If the alarm is reported against a TCC2 card, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Step 3 If the alarm is reported against an OC-N card, complete the "Reset a Traffic Card in CTC" procedure on page 2-250.

Step 4 If the alarm is reported against an XC card, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the XC card. (The process is similar.)

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252.

Step 6 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting card.

Step 7 If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for instructions.

Step 8 If the alarm does not clear, reseat the power cable connection to the connector. For more information about power connections, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 9 If the alarm does not clear, physically replace the power cable connection to the connector.

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.287 PWR-FAIL-B

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), XC card, OC-N cards, or TCC2 card.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.**

Clear the PWR-FAIL-B Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-195.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.288 PWR-FAIL-RET-A

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, XC card, OC-N cards, or TCC2 card.

Clear the PWR-FAIL-RET-A Alarm:

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-195.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.289 PWR-FAIL-RET-B

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, XC card, OC-N cards, or TCC2 card.

Clear the PWR-FAIL-RET-A Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-195.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.290 RAI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

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

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-24.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.291 RCVR-MISS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object:DS1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from a DS-1 port, or a possible mismatch of backplane equipment occurs. For example, an SMB connector or a BNC connector might be misconnected to a DS-1 card.

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

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

Clear the RCVR-MISS Alarm

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

Step 2 If the attachment is okay, verify that the cabling is securely connected.

Step 3 If the cabling is okay, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the receive cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.292 RFI

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Remote Failure Indication condition is similar to the "RFI-L" condition on page 2-199 but it is raised against an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card when it has the "AIS" condition on page 2-24. The MXP or TXP cards will only raise AIS (or RFI) when they are in line or section termination mode, that is, when the MXP or TXP cards in line termination mode or section termination mode has improperly terminated overhead bytes.

Clear the RFI Condition

Step 1 Complete the "Delete a Circuit" procedure on page 2-254 and then recreate the circuit.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.293 RFI-L

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

A Remote Fault Indication (RFI) Line condition occurs when the ONS 15454 detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

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

Step 2 Identify and clear any alarms, particularly the "LOS (OCN)" alarm on page 2-144.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.294 RFI-P

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

RFI Path condition occurs when the ONS 15454 detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS-NR) on the reporting ONS 15454:

a. Confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as IS.

e. If the admin state column lists the port as OOS,MT or OOS,DSLBD, click the column and choose **IS**. Click **Apply**.

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

Step 3 Clear alarms in the node with the failure, especially the "UNEQ-P" alarm on page 2-231 or the "UNEQ-V" alarm on page 2-233.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.295 RFI-V

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: VT-TERM

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

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

Clear the RFI-V Condition

Step 1 Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 2 If connectors are correctly connected, verify that the DS-1 port is active and in service (IS-NR):

a. Confirm that the LED is correctly illuminated on the physical card:

b. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

c. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

e. Verify that the admin state column lists the port as IS.

f. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 3 If the ports are active and in service, use an optical test set to verify that the signal source does not have errors.

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

Step 4 If the signal is valid, log into the node at the far-end of the reporting ONS 15454.

Step 5 Clear alarms in the far-end node, especially the "UNEQ-P" alarm on page 2-231 or the "UNEQ-V" alarm on page 2-233.

Step 6 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.296 RING-ID-MIS

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: OCN, OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to BLSR RING-MISMATCH, but rather than apply to ring protection, RING-ID-MIS applies to DWDM node discovery within the same network.

Clear the RING-ID-MIS Alarm

Step 1 Complete the "Clear the RING-MISMATCH Alarm" procedure on page 2-201.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.297 RING-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

A Procedural Error Mismatch Ring alarm occurs when the ring name of the ONS 15454 node that is reporting the alarm does not match the ring name of another node in the BLSR. Nodes connected in a BLSR must have identical ring names to function. This alarm can occur during BLSR provisioning.

RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.

Clear the RING-MISMATCH Alarm

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 Note the number in the Ring Name field.

Step 3 Log into the next ONS 15454 node in the BLSR.

Step 4 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-241.

Step 5 If the ring name matches the ring name in the reporting node, repeat Step 4 for the next ONS 15454 in the BLSR.

Step 6 Complete the "Change a BLSR Ring Name" procedure on page 2-241.

Step 7 Verify that the ring map is correct.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.298 RING-SW-EAST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR using a Force Ring command. The condition clears when the switch is cleared.

Note RING-SW-EAST is an informational condition and does not require troubleshooting.

2.8.299 RING-SW-WEST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR using a Force Ring command. The condition clears when the switch is cleared.

Note RING-SW-WEST is an informational condition and does not require troubleshooting.

2.8.300 RSVP-HELLODOWN

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UCP-NBR

The Resource Reservation Protocol (RSVP) Hello Down alarm occurs when the Hello protocol, which monitors UCP control channel status, is not available for reserving resources. The lack of availability can be caused by misconfiguration or loss of connectivity between the reporting node and its neighbor.

Clear the RSVP-HELLODOWN Alarm

Step 1 Ensure that there are no physical layer problems between the reporting node and its neighbor.

Step 2 Ensure that neighbor discovery (if enabled) has completed without any errors:

a. In the node CTC view, click the **Provisioning > UCP > Neighbor** tabs.

b. Look for the neighbor ID and address. If it is present, neighbor discovery is working.

Step 3 Ensure that RSVP hello is enabled on the neighbor node. If the neighbor is a Cisco ONS 15454, use the following procedure to ensure that RSVP Hello is enabled on the neighbor. If not, use the corresponding procedure on the core network element:

a. In node view, click **View > Go to Network View**.

b. Double-click the neighbor node in the network map.

c. Click the **Provisioning > UCP > Node** tabs on this neighbor.

d. Ensure that the RSVP area of the window contains entries in the Restart Time, Retransmit Interval, Recovery Time, and Refresh Interval fields.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.301 RUNCFG-SAVENEED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML1000 and ML100T cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering the **copy run start** command at the CLI. If you do not save the change, the change is lost after the card reboots.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.302 SD (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Signal Degrade (SD) condition occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal degrade threshold. The alarm applies to the card ports (CLIENT) and the trunk carrying optical or electrical signals to the card.

Signal degrade is defined by Telcordia as a soft failure condition. SD and SF both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. The BER threshold on the ONS 15454 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}.

Clear the SD (TRUNK) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.303 SD (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Signal Degrade (SD) condition for DS-1 or DS-3 occurs when the quality of an electrical signal has exceeded the BER signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and also signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

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

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT) but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G cross-connect card switches that in turn can cause switching on the lines or paths.

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

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

Note Some levels of BER errors (such as 10E_9) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 10E_9 rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SONET ONS electrical cards is the Omniber 718.

Clear the SD (DS1, DS3) Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-254.

Step 2 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.

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

Step 4 If the optical power level is okay, verify that optical receive levels are within the acceptable range.

Step 5 If receive levels are okay, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 9 Verify that a single-mode laser is used at the far end.

Step 10 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.11.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-251.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 11 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.304 SD-L

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SD Line condition is similar to the "SD (DS1, DS3)" condition on page 2-203. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The alarm is superseded by higher-priority alarms such as the "LOF (EC1-12)" alarm on page 2-134, the "LOF (OCN)" alarm on page 2-134, the "LOS (EC1-12)" alarm on page 2-141, and the "LOS (OCN)" alarm on page 2-144.

Clear the SD-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.305 SD-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SD Path condition is similar to the "SD (DS1, DS3)" condition on page 2-203, but it applies to the path (STS) layer of the SONET overhead. A path or ST-level SD alarm travels on the B3 byte of the SONET overhead.

For path protected circuits, the BER threshold is user provisionable and has a range for SD from 10^{-9} to 10^{-5}. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6}.

On path protection, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal degrade and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. SD causes the card to switch from working to protect. The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.306 SD-V

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VT-MON

An SD-V condition is similar to the "SD (DS1, DS3)" condition on page 2-203, but it applies to the VT layer of the SONET overhead.

For path protected circuits, the BER threshold is user provisionable and has a range for SD from 10^{-9} to 10^{-5}. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6}.

On path protection configurations, an SD-V condition does not cause a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-V condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal degrade and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. SD causes the card to switch from working to protect. The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-V Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.307 SF (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Signal Failure (SF) for the CLIENT or TRUNK occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal fail threshold. The alarm applies to the card ports (CLIENT) and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a soft failure condition. SF monitors the incoming BER and is triggered when the BER surpasses the default range.

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

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

Clear the SF (TRUNK) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.308 SF (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Signal Fail (SF) condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a "hard failure" condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

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

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

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

Clear the SF (DS1, DS3) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.309 SF-L

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SF Line condition is similar to the "SF (DS1, DS3)" condition on page 2-207, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

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

The alarm is superseded by higher-priority alarms such as the "LOF (EC1-12)" alarm on page 2-134, the "LOF (OCN)" alarm on page 2-134, the "LOS (EC1-12)" alarm on page 2-141, or the "LOS (OCN)" alarm on page 2-144.

Clear the SF-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.310 SF-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SF Path condition is similar to an "SF-L" condition on page 2-208, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

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

Clear the SF-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.311 SF-V

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VT-MON

An SF-V condition is similar to the "SF (DS1, DS3)" condition on page 2-207, but it applies to the VT layer of the SONET overhead.

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-204.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.312 SFTWDOWN

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2 is downloading or transferring software.

If the active and standby TCC2s have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2.

If the active and standby TCC2s have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2 reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note SFTWDOWN is an informational alarm.

2.8.313 SH-INS-LOSS-VAR-DEG-HIGH

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Switch Insertion Loss Variation Degrade High alarm occurs as the OSC-CSM card optical switch ages and slowly increases its insertion loss. This alarm indicates that the insertion loss has crossed the high degrade threshold. The card will need to be replaced eventually.

2.8.313.1 Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 as appropriate.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.314 SH-INS-LOSS-VAR-DEG-LOW

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Switch Insertion Loss Variation Degrade Low alarm occurs as the OSC-CSM card optical switch ages and slowly decreases its insertion loss. This alarm indicates that the insertion loss has crossed the low degrade threshold. The card will need to be replaced eventually.

2.8.314.1 Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm

Step 1 For the alarmed card, complete the "Physically Replace a Traffic Card" procedure on page 2-252 as appropriate.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.315 SHUTTER-OPEN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The SHUTTER-OPEN alarm occurs if an OSC-CSM card laser shutter remains open after the "LOS (OTS)" alarm on page 2-146 is detected. A laser shutter remains open if an optical safety issue is present and closes when the OSC-CSM card LINE-RX port receives OSC power for three consecutive seconds.

Clear the SHUTTER-OPEN Alarm

Step 1 Complete the "Clear the LOS (OTS) Alarm" procedure on page 2-146.

Step 2 If the SHUTTER-OPEN alarm still does not clear, it indicates that the unit shutter is not working properly. Complete the "Physically Replace a Traffic Card" procedure on page 2-252.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.316 SIGLOSS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FC, FCMR, GE, ISC,TRUNK

The Signal Loss on Data Interface alarm is raised on FM_MR-4 card receive client ports when there is an LOS. The alarm demotes the SYNCLOSS alarm.

Clear the SIGLOSS Alarm

Step 1 Ensure that the Fibre Channel data port connection at the near-end card port of the SONET link is operational.

Step 2 Verify fiber continuity to the port.

Step 3 Check the physical port LED on the Fibre Channel card. The port LED looks clear (that is, not lit green) if the link is not connected.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.317 SNTP-HOST

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15454 serving as an IP proxy for the other ONS 15454s in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which could affect the SNTP server/router connecting to the proxy ONS system.

Step 3 If no network problems exist, ensure that the ONS system proxy is provisioned correctly:

- **a.** In node view for the ONS 15454 serving as the proxy, click the **Provisioning > General** tabs.
- **b.** Ensure that the Use NTP/SNTP Server check box is checked.
- **c.** If the Use NTP/SNTP Server check box is not checked, click it.
- **d.** Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.318 SPAN-SW-EAST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared.

Note SPAN-SW-EAST is an informational condition and does not require troubleshooting.

2.8.319 SPAN-SW-WEST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared.

Note SPAN-SW-WEST is an informational condition and does not require troubleshooting.

2.8.320 SQUELCH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The "AIS-P" condition on page 2-25 also appears on all nodes in the ring except the isolated node.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right 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 (IS-NR) for the laser to be on. The laser is off when the safety key is off (labeled 0).**

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

Clear the SQUELCH Condition

Step 1 Determine the isolated node:

a. In node view, click **View > Go to Network View**.

b. The grayed out node with red spans is the isolated node.

Step 2 Verify fiber continuity to the ports on the isolated node.

Step 3 If fiber continuity is okay, verify that the proper ports are in service:

a. Confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

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

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

d. Verify that the admin state column lists the port as IS.

e. If the admin state column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 4 If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 5 If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.

Step 6 If the receiver levels are okay, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are okay, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the OC-N card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 8 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.321 SQUELCHED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EC1-12, ESCON, FC, GE, ISC, OCN, TRUNK

The CLIENT Signal Squelched alarm is raised by an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card when ITU-T G.709 monitoring is enabled and the card is operating in transparent mode. The alarm occurs on a far-end MXP or TXP card client port when the near end detects the "LOF (OCN)" alarm on page 2-134 or the "LOS (OCN)" alarm on page 2-144. The signal loss is indicated by the "OTUK-AIS" alarm on page 2-183 in the OTN overhead. SQUELCHED can also indicate that the far-end trunk signal is invalid.

Clear the SQUELCHED Alarm

Step 1 Verify that the far-end node and near-end node are not reporting the "LOF (OCN)" alarm on page 2-134 or the "LOS (OCN)" alarm on page 2-144. If so, complete the "Clear the LOF (OCN) Alarm" procedure on page 2-135.

Step 2 If no LOF or LOS is reported, verify that the far-end node and near-end are not reporting the trunk "WVL-MISMATCH" alarm on page 2-238 or the "DSP-FAIL" alarm on page 2-68. If either alarm is reported, complete the "Clear the WVL-MISMATCH alarm" procedure on page 2-238 or the "Clear the DSP-FAIL Alarm" procedure on page 2-68 as appropriate.

Step 3 If no WVL-MISMATCH or DSP-FAIL is reported, verify that the near-end port reporting the SQUELCHED alarm is in service and is not in loopback:

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

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

c. If the port admin state column says OOS,MT or OOS,DSBLD, click the cell to highlight it and choose **IS** from the drop-down list. Changing the state to IS also clears any loopback provisioned on the port.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.322 SQM

- Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM
- Default Severity: Major (MJ), Service-Affecting (SA) for VT-TERM
- Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

Step 1 For the errored circuit, complete the "Delete a Circuit" procedure on page 2-254.

Step 2 Recreate the circuit using the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.323 SSM-DUS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The Synchronization Status (SSM) Message Quality Changed to DUS condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

Note SSM-DUS is an informational condition and does not require troubleshooting.

2.8.324 SSM-FAIL

- Single Failure Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Double Failure Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: BITS, DS1, OCN, TRUNK

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

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM.

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

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.325 SSM-LNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.

Note SSM-LNC is an informational condition and does not require troubleshooting.

2.8.326 SSM-OFF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS system is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-216.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.327 SSM-PRC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level is changed to PRC.

Note SSM-PRC is an informational condition and does not require troubleshooting.

2.8.328 SSM-PRS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note SSM-PRS is an informational condition and does not require troubleshooting.

2.8.329 SSM-RES

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

Note SSM-RES is an informational condition and does not require troubleshooting.

2.8.330 SSM-SDN-TN

The SSM-SDN-TN condition is not used in this platform in this release. It is reserved for future development.

2.8.331 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for future development.

2.8.332 SSM-SMC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

Note SSM-SMC is an informational condition and does not require troubleshooting.

2.8.333 SSM-ST2

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

Note SSM-ST2 is an informational condition and does not require troubleshooting.

2.8.334 SSM-ST3

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

Note SSM-ST3 is an informational condition and does not require troubleshooting.

2.8.335 SSM-ST3E

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.

Note SSM-ST3E is an informational condition and does not require troubleshooting.

2.8.336 SSM-ST4

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note SSM-ST4 is an informational condition and does not require troubleshooting.

2.8.337 SSM-STU

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

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

Clear the SSM-STU Condition

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Complete one of the following depending upon the status of the Sync Messaging Enabled check box:

- If the **Sync Messaging Enabled** check box for the BITS source is checked, uncheck the box.
- If the **Sync Messaging Enabled** check box for the BITS source is not checked, check the box.

Step 3 Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.338 SSM-TNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

Note SSM-TNC is an informational condition and does not require troubleshooting.

2.8.339 SWMTXMOD

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

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

If the alarm reports against a cross-connect card, it occurs when a logic component internal to the reporting cross-connect card is OOF with a second logic component on the same cross-connect card. One or more traffic cards could lose traffic as a result of the cross-connect frame failure.

In R4.7, the alarm initiates an autonomous switch in 1+1, 1:1, 1:N, path protection, and BLSR protection schemes if it is raised on the following I/O cards: DS-1, DS3-E, DS3-CR, OC-12, OC-48 IR, OC-48 ELR, and OC3-4. The switching time is greater than 60 milliseconds and typically lasts approximately 500 milliseconds.

If the alarm is raised against active XCVT card, an autonomous switch to the standby XCVT occurs under the following circumstances:

- The standby XCVT does not have an SWMTXMOD alarm active.
- No lockout condition is present on the XCVT card.

If the standby XCVT does has an active SWMTXMOD alarm, the XC switch request from CTC or TL1 is denied.

Clear the SWMTXMOD Alarm

Step 1 If the card reporting the alarm is the standby XC cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the standby cross-connect card.

Step 4 If the card reporting the alarm is the active cross-connect card, complete the "Side Switch the Active and Standby XC10G Cross-Connect Cards" procedure on page 2-251.

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

Step 5 If the card reporting the alarm is not the active cross-connect card or if you completed the side switch in Step 4, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 7 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the standby cross-connect card.

Step 8 If the card reporting the alarm is a traffic card, complete the "Side Switch the Active and Standby XC10G Cross-Connect Cards" procedure on page 2-251.

Step 9 If the alarm does not clear, complete the "Reset a Traffic Card in CTC" procedure on page 2-250 for the reporting card. For the LED behavior, see the "2.10.2 Typical Traffic Card LED Activity During Reset" section on page 2-240.

Step 10 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 11 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-252 for the traffic line card.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.340 SWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

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

Note SWTOPRI is an informational condition and does not require troubleshooting.

2.8.341 SWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

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.

Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-223.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.342 SWTOTHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

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.

Clear the SWTOTHIRD Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-223 or the "SYNCSEC" alarm on page 2-223.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.343 SYNC-FREQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The Synchronization Reference Frequency Out of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Clear the SYNC-FREQ Condition

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency.

For specific procedures to use the test set equipment, consult the manufacturer. For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

Step 2 If the reference source frequency is not outside of bounds, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the TCC2.

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

Note It takes up to 30 minutes for the TCC2 to transfer the system software to the newly installed TCC2. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2 reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ condition continues to report after replacing the TCC2 card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.344 SYNCLOSS

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Objects: FC, FCMR, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 cards when there is a loss of signal synchronization on the client port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

Step 1 Complete the "Clear the SYNCLOSS Alarm" procedure on page 2-223.

Step 2 If the SYNCLOSS alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.345 SYNCPRI

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the "SWTOSEC" alarm on page 2-221.

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration for the REF-1 of the NE Reference.

Step 3 If the primary timing reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-139.

Step 4 If the primary reference clock is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.346 SYNCSEC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to the third timing source also triggers the "SWTOTHIRD" alarm on page 2-221.

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration of the REF-2 for the NE Reference.

Step 3 If the second reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-139.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.347 SYNCTHIRD

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

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 TCC2 card might have failed. The ONS 15454 often reports either the "FRNGSYNC" condition on page 2-103 or the "HLDOVRSYNC" condition on page 2-116 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 edge of the shelf assembly.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify that the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-139.

Step 4 If the third timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 5 If the third timing source uses the internal ONS system timing, complete the "Reset an Active TCC2 and Activate the Standby Card" procedure on page 2-250.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete "Remove and Reinsert (Reseat) the Standby TCC2 Card" procedure on page 2-251. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-252.

2.8.348 SYSBOOT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2 card. No action is required. The alarm clears when all cards finish rebooting the new software.The reboot takes up to 30 minutes.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.8.349 TIM

- Default Severity: Critical (CR), Service-Affecting (SA) for TRUNK
- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA) for OCN
- Logical Objects: OCN, TRUNK

The Section Trace Identifier Mismatch (TIM) occurs when the expected J0 section trace string does not match the received section trace string.

If the condition occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Follow the procedure below to clear either instance.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (OCN)" alarm on page 2-144 or the "UNEQ-P" alarm on page 2-231. If these alarms accompany TIM, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm or Condition

Step 1 Log into the circuit source node and click the **Circuits** tab.

Step 2 Select the circuit reporting the condition, then click **Edit**.

Step 3 In the Edit Circuit window, check the **Show Detailed Map** box.

Step 4 On the detailed circuit map, right-click the source circuit port and choose **Edit J1 Path Trace (port)** from the shortcut menu.

Step 5 Compare the Current Transmit String and the Current Expected String entries in the Edit J1 Path Trace dialog box.

Step 6 If the strings differ, correct the Transmit or Expected strings and click **Apply**.

Step 7 Click **Close**.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem if necessary.

2.8.350 TIM-MON

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN, TRUNK

The Section Monitor Trace Identifier Mismatch alarm is similar to the "TIM-P" alarm on page 2-226, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In Transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or vice versa.)

Clear the TIM-MON Alarm

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-227.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.351 TIM-P

- Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM
- Default Severity: Minor (MN), Non-Service Affecting (NSA) for STSMON
- Logical Objects: STSMON, STSTRM

The TIM Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

TIM-P also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. TIM-P is usually accompanied by other alarms, such as the "LOS (OCN)" alarm on page 2-144, the "UNEQ-P" alarm on page 2-231, or the "PLM-P" alarm on page 2-190. If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

Clear the TIM-P Alarm

Step 1 Complete the "Clear the TIM Alarm or Condition" procedure on page 2-225.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447). If the alarm applies to the STSTRM object, it is service-affecting.

2.8.352 TPTFAIL (FCMR)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel (FC) port on an FC_MR-4 card when the port receives another SONET error such as AIS-P, LOP-P, UNEQ-P, PLM-P, TIM-P, LOM (for VCAT only), or SQM (for VCAT only). This TPTFAIL can also be raised against Fibre Channel cards if the remote FC card port is down from INC-SIG-LOSS or INC-SYNC-LOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm).

Clear the TPTFAIL (FCMR) Alarm

Step 1 Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.353 TPTFAIL (G1000)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

The Transport (TPT) Layer Failure alarm for the G-Series Ethernet cards indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the "AIS-P" alarm on page 2-25, the "LOP-P" alarm on page 2-136, the "PDI-P" alarm on page 2-188, or the "UNEQ-P" alarm on page 2-231 exist on the SONET path used by the Ethernet port, the affected port

causes a TPTFAIL alarm. Also, if the far-end G1000-4 port Ethernet port is administratively disabled or it is reporting the "CARLOSS (G1000)" alarm on page 2-49, the C2 byte in the SONET path overhead indicates the "PDI-P" alarm on page 2-188, which in turn causes a TPTFAIL to be reported against the near-end port.

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

An occurrence of TPTFAIL on an ONS 15454 G1000-4 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-4 port that is mapped to the port.

Clear the TPTFAIL (G1000) Alarm

Step 1 Clear any alarms being reported by the OC-N card on the G1000-4 circuit.

Step 2 If no alarms are reported by the OC-N card, or if the "PDI-P" condition on page 2-188 is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.354 TPTFAIL (ML1000, ML100T, ML2)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: ML1000, ML100T, ML2

The TPT Layer Failure alarm for the ML-Series Ethernet cards indicates a break in the end-to-end POS link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the "AIS-P" condition on page 2-25, the "LOP-P" alarm on page 2-136, the "PDI-P" condition on page 2-188, or the "UNEQ-P" alarm on page 2-231 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML POS port is administratively disabled, it inserts an "AIS-P" condition on page 2-25 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Note The ML2 object is currently used only in the ONS 15310 platform and is reserved for future development in the ONS 15454 platform.

Clear the TPTFAIL (ML1000, ML100T, ML2) Alarm

Step 1 If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 2 If the "PLM-P" alarm on page 2-190 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 3 If the "PDI-P" condition on page 2-188 is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a "CARLOSS (G1000)" alarm on page 2-49 is reported against the G-Series card, and if so, complete the "Clear the CARLOSS (G1000) Alarm" procedure on page 2-50.

Step 4 If the "AIS-P" alarm on page 2-25, the "LOP-P" alarm on page 2-136, or the "UNEQ-P" alarm on page 2-231 is present, clear those alarms using the procedures in those sections.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.355 TRMT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object:DS1

A Missing Transmitter alarm occurs when there is a transmit failure on the ONS 15454 DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the reporting DS-1 card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.356 TRMT-MISS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card. For example, an SMB connector or a BNC connector might be connected to a DS-1 card instead of a DS-3 card.

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

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the DS-1 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.357 TX-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: DS1

The (TX) Transmit Direction AIS condition is raised by the ONS backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

Step 1 Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-144, or OOS ports.

Step 2 Clear the downstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.358 TX-RAI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object:DS1

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

Step 1 Complete the "Clear the TX-AIS Condition" procedure on page 2-230.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.359 UNC-WORD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Uncorrected FEC Word condition indicates that the forward error correction (FEC) capability could not sufficiently correct the frame.

FEC allows the system to tolerate a 7- to 8-dB reduction in signal-to-noise ratio (SNR).

Clear the UNC-WORD Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-205.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.360 UNEQ-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A signal label mismatch fault (SLMF) UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note If a newly created circuit has no signal, an UNEQ-P alarm is reported on the OC-N cards and the "AIS-P" condition on page 2-25 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 edge of the shelf assembly.

Clear the UNEQ-P Alarm

Step 1 In node view, click **View > Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7.

Step 6 If the Type column does contain VTT, attempt to delete these row(s):

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a. Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-254.

b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

c. If any other rows contain VTT, repeat Step 6.

Step 7 If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:

a. Click the **Circuits** tab.

b. Verify that PARTIAL is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic.

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

Step 9 If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.

Complete the "Delete a Circuit" procedure on page 2-254.

Step 10 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

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

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

Step 13 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the OC-N and DS-N cards.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

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

Step 14 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.361 UNEQ-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is the node that is transmitting the VT-level signal into the node reporting the UNEQ-P. The problem node is the next node upstream that processes the signal at the VT level. The V in UNEQ-V indicates that the failure has occurred at the VT layer.

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

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

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

Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-232.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.362 UNREACHABLE-TARGET-POWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCH

The Unreachable Port Target Power alarm occurs on WSS32 cards during startup as the card laser attains its correct power level. The condition disappears when the card successfully boots.

Note UNREACHABLE-TARGET-POWER is an informational condition. It only requires troubleshooting if it does not clear.

2.8.363 UT-COMM-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Universal Transponder (UT) Module Communication Failure alarm is raised on MXP_2.5G_10E and TXP_MR_10E cards when there is a universal transponder communication failure because the UT has stopped responding to the TCC2.

Clear the UT-COMM-FAIL Alarm

Step 1 Double-click the card to display the card view.

Step 2 Request a laser restart:

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

b. Check the Request Laser Restart check box.

c. Click **Apply**.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.364 UT-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Universal Transponder Module Hardware Failure alarm is raised against MXP_2.5G_10E and TXP_MR_10E cards when a UT-COMM-FAIL alarm persists despite being reset.

Clear the UT-FAIL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the alarmed card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.365 VCG-DEG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the "OOU-TPT" alarm on page 2-179. It only occurs when a critical alarm, such as LOS, causes a signal loss.

Clear the VCG-DEG Condition

Step 1 Look for and clear any critical alarms that apply to the errored card, such as "LOS (2R)" alarm on page 2-139 or "LOS (OTS)" alarm on page 2-146.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.366 VCG-DOWN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when both member circuits carried by the ML-Series Ethernet card are down. This alarm occurs in conjunction with another critical alarm, such as the "LOS (2R)" alarm on page 2-139.

Clear the VCG-DOWN Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-235.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.367 VOA-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Degrade alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high degrade threshold. The alarmed card should be replaced at the next opportunity.

Clear the VOA-HDEG Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the alarmed card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.368 VOA-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Fail alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high fail threshold. The card must be replaced.

Clear the VOA-HFAIL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the alarmed card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.369 VOA-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Degrade alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low degrade threshold. The alarmed card should be replaced at the next opportunity.

Clear the VOA-LDEG Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the alarmed card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.370 VOA-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Fail alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low fail threshold. The card must be replaced.

Clear the VOA-LFAIL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-252 for the alarmed card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.371 WKSWPR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Working Switched To Protection condition occurs when a line experiences the "LOS (OCN)" alarm on page 2-144, the "SF (DS1, DS3)" condition on page 2-207, or the "SD (TRUNK)" condition on page 2-203.

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOS (OCN) Alarm" procedure on page 2-145.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.372 WTR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Wait To Restore condition occurs when the "WKSWPR" condition on page 2-237 is raised, but the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic is switched back to the working path.

Caution DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.

Note WTR is an informational condition and does not require troubleshooting.

2.8.373 WVL-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Equipment Wavelength Mismatch alarm applies to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

Clear the WVL-MISMATCH alarm

Step 1 In node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card to display the card view.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 In the Wavelength field, view the provisioned card wavelength.

Step 4 If you have access to the site, compare the wavelength listed on the card faceplate with the provisioned wavelength. If you are remote, compare this wavelength with the card identification in the inventory:

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

b. Locate the slot where the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card is installed and view the card wavelength in the name.

Step 5 If the card was provisioned for the wrong wavelength, double-click the card in node view to display the card view.

Step 6 Click the **Provisioning > Card** tabs.

Step 7 In the Wavelength field, click the drop-down list and choose the correct wavelength.

Step 8 Click **Apply**.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.9 DWDM Card LED Activity

ONS 15454 DWDM card LED activity differs from typical traffic card LED activity. The following sections list the DWDM card LED sequences during card insertion and reset.

2.9.1 DWDM Card LED Activity After Insertion

When an DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.
6. The SF LED stays illuminated until all card ports connect to their far-end counterparts and a signal is present.

2.9.2 DWDM Card LED Activity During Reset

When an DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.
2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters “LDG” appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

2.10 Traffic Card LED Activity

ONS 15454 traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

2.10.1 Typical Traffic Card LED Activity After Insertion

When a non-DWDM card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

2.10.2 Typical Traffic Card LED Activity During Reset

While a non-DWDM card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters “LDG” appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

2.10.3 Typical Card LED State After Successful Reset

When a non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials “SBY,” and this has replaced the white “LDG” depiction on the card in CTC.
- If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials “ACT,” and this has replaced the white “LDG” depiction on the card in CTC.

2.10.4 Typical Cross-Connect LED Activity During Side Switch

While an XC10G cross-connect card is switched in CTC from active (ACT) to standby (SBY) or vice versa, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

2.11 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 documentation. They are included in this chapter for the user’s convenience. For further information, please refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

2.11.1 Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Note For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Change a BLSR Ring Name

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, enter the new name in the Ring Name field.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, right-click the node on the ring map.

Step 6 Select **Set Node ID** from the shortcut menu.

Step 7 In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.

Step 8 Click **OK**.

Verify Node Visibility for Other Nodes

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > BLSR** tabs.

Step 3 Highlight a BLSR.

Step 4 Click **Ring Map**.

Step 5 In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.

Step 6 Click **Close**.

2.11.2 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Note A Force switch will switch traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch will not switch traffic on a protect path. A Force switch preempts a Manual switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group will say "Force to working."

Initiate a 1+1 Protection Port Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual switch will switch traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group will say "Force to working."

Clear a 1+1 Protection Port Force or Manual Switch Command

Note If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear**.

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic will immediately revert to the working port if the group was configured for revertive switching.

Initiate a Card or Port Lock On Command

Note For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active card where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lock Out Command

Note For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lockout.

Step 3 In the Selected Group list, click the card you want to lock traffic out of.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Card or Port Lock On or Lock Out Command

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate a 1:1 Card Switch Command

Note The Switch command only works on the Active card, whether it is Working or Protect. It does not work on the Standby card.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 3.

Step 2 Click **View > Go to Network View**.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform path protection span switching** field.

Step 5 Choose **FORCE SWITCH AWAY** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits will not switch.

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform path protection span switching** field.

Step 4 Choose **MANUAL** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is MANUAL. Unprotected circuits will not switch.

Initiate a Lock Out of Protect-Switch for All Circuits on a Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.

Caution The Lock Out of Protect command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform path protection span switching** field.

Step 4 Choose **LOCK OUT OF PROTECT** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits will not switch.

Clear Path Protection Span External Switching Command

Note If the ports terminating a span are configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

a. Click the **Perform path protection span switching** field.

b. Choose **CLEAR** from the drop-down list.

c. Click **Apply**.

d. In the Confirm Path Protection Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is CLEAR. Unprotected circuits will not switch.

Initiate a Force Switch a BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you will switch, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Force Span Switch a Four-Fiber BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you will switch, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Manual Ring Switch on a BLSR

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Lock Out on a BLSR Protect Span

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **LOCKOUT PROTECT SPAN** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate an Exercise Ring Switch on a BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you will exercise, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Initiate an Exercise Ring Switch on a Four Fiber BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you will exercise, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Clear a BLSR External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the BLSR you want to clear.

Step 5 Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

2.11.3 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2 cards, and cross-connect cards.

Caution For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Caution Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.

Step 3 Right-click the card. Choose **Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Reset an Active TCC2 and Activate the Standby Card

Caution Resetting an active TCC2 card reset can be traffic-affecting.

Note Before you reset the TCC2, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active TCC2 card:

If you are looking at the physical ONS shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.

Step 3 Right-click the active TCC2 in CTC.

Step 4 Choose **Reset Card** from the shortcut menu.

Step 5 Click **Yes** in the Confirmation Dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "2.10.3 Typical Card LED State After Successful Reset" section on page 2-240.

Step 7 Double-click the node and ensure that the reset TCC2 is in standby mode and that the other TCC2 is active. Verify the following:

- If you are looking at the physical ONS shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
- No new alarms appear in the Alarms window in CTC.

Side Switch the Active and Standby XC10G Cross-Connect Cards

Caution The cross-connect card side switch is traffic-affecting.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Display node view.

Step 3 Determine the active or standby XC10G cross-connect card.

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

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

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the "2.10.4 Typical Cross-Connect LED Activity During Side Switch" section on page 2-240 for LED information.

2.11.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating, resetting, and replacing TCC2, cross-connect, and traffic cards.

Caution Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242. In-depth traffic switching procedures and information can be found in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Remove and Reinsert (Reseat) the Standby TCC2 Card

Caution Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).

Caution The TCC2 reseat might be traffic-affecting. Refer to the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for traffic-switching procedures.

Note Before you reset the TCC2 card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note When a standby TSC card is removed and reinserted (reseated), all three fan lights might momentarily illuminate, indicating that the fan TCC2s have also reset.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Ensure that theTCC2 you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

Step 2 When the TCC2 is in standby mode, unlatch both the top and bottom ejectors on the TCC2.

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 ejectors.

Note The TCC2 will take several minutes to reboot and will display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about LED behavior during card rebooting.

Remove and Reinsert (Reseat) Any Card

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Physically Replace a Traffic Card

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for commonly used procedures.

Step 1 Open the card ejectors.

Step 2 Slide the card out of the slot.

Step 3 Open the ejectors on the replacement card.

Step 4 Slide the replacement card into the slot along the guide rails.

Step 5 Close the ejectors.

Physically Replace an In-Service Cross-Connect Card

Caution The cross-connect reseat might be traffic-affecting. Refer to the "2.11.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-242 for traffic-switching procedures prior to completing this procedure.

Step 1 Determine the active cross-connect card (XCVT/XC10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

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

Step 2 Switch the active cross-connect card (XCVT/XC10G) to standby:

a. In the node view, click the **Maintenance > Cross-Connect** tabs.

b. Under Cross Connect Cards, choose **Switch**.

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

Note After the active 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 3 Physically remove the new standby cross-connect card (XCVT/XC10G) from the ONS 15454.

Note An improper removal (IMPROPRMVL) alarm is raised when a card reseat is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card replacement is complete.

Step 4 Insert the replacement cross-connect card (XCVT/XC10G) into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

2.11.5 Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the card reporting the alarm to display the card view.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column on the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

Step 5 If the entry is consistent with the original provisioning, go back to your original procedure.

Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

Step 7 Click **Apply**.

Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

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

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node SDCC Terminations

Note Portions of this procedure are different for ONS 15454 DWDM nodes.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > Comm Channels > SDCC** tab.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

a. Click **Create**.

b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c. In the port state area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Clear an OC-N Card Facility or Terminal Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

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

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the admin state column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an OC-N Card XC Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

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

Step 4 Uncheck the XC Loopback check box.

Step 5 Click **Apply**.

Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance > DS3** tabs or the **Maintenance > DS1** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the admin state column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks

Note This procedure does not apply to DS3XM-6 or DS3XM-12 cards.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

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

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the admin state column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an MXP, TXP, or FCMR Card Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

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

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the admin state column, determine whether any port row shows an admin state other than IS, for example, OOS,MT.

Step 7 If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an Ethernet Card Loopback Circuit

This procedure applies to CE_100T-8 cards.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

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

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the admin state column, determine whether any port row shows a state other than IS, for example, OOS,MT.

Step 7 If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

2.11.6 Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

Step 1 Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.

Step 2 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that might have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly:

a. Open the front door of the shelf assembly. If it is already open or if the shelf assembly does not have a front door, continue with Step 3.

- Open the front door lock.
- Press the door button to release the latch.
- Swing the door open.

b. Remove the front door (optional):

- 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 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 5 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 6 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.

Step 7 Visually inspect the air filter material for dirt and dust.

Step 8 If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.

Caution Do not put a damp filter back in the ONS 15454.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

Note On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

Step 14 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15454.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

Note The 15454-SA-ANSI or 15454-SA-HD shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 OC-192 and OC-48 AS cards.

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

Step 1 Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with Step 3.

a. Open the front door lock.

b. Press the door button to release the latch.

c. Swing the door open.

Step 2 Remove the front door (optional):

a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

c. Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Fold out the retractable handles at the outside edges of the fan tray.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

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 "Inspect, Clean, and Replace the Reusable Air Filter" section on page 2-257.

Step 8 Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 9 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Step 10 If you replace the door, be sure to reattach the ground strap.

2.11.7 Interface Procedures

This section includes instructions for replacing an ONS 15454 EIA and an ONS 15454 AIP.

Replace the Electrical Interface Assembly

Note You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

Step 1 To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.

Note If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

Step 3 If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.

Step 4 If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.

Note Attach backplane sheet metal covers whenever EIAs are not installed.

Step 5 Line up the connectors on the new EIA with the mating connectors on the backplane.

Step 6 Gently push the EIA until both sets of connectors fit together snugly.

Step 7 Replace the nine perimeter screws that you removed while removing the backplane cover.

Step 8 If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

Step 9 Reattach the lower backplane cover.

Replace the Alarm Interface Panel

Caution Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.

Caution If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Assistance Center (TAC) at 1 800 553-2447 when prompted to do so in the procedure.

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

Note Perform this procedure during a maintenance window. Resetting the active TCC2 card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC2 card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Caution Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC (1 800 553-2447).

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 will be affected.

You need a #2 Phillips screwdriver.

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

a. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.

b. If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.

Step 2 Record the MAC address of the old AIP:

a. Log into the node where you will replace the AIP. For login procedures, see the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

b. In node view, click the **Provisioning > Network** tabs.

c. Record the MAC address shown in the General tab.

Step 3 Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place.

Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so will cause a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning > Network** tabs.

Caution Cisco recommends TCC2 card resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby TCC2 card:

a. Right-click the standby TCC2 card and choose **Reset Card**.

b. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.

Note The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active TCC2 card:

a. Right click the active TCC2 card and choose **Reset Card**.

b. Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication will appear on the card in CTC.

Note The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down list, choose **Exit** to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

a. In node view, click the **Provisioning > Network** tabs.

b. Record the MAC address shown in the General tab.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Step 24 The Node MAC Addresses dialog box appears:

a. From the Node drop-down list, 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**.

Step 25 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

Note The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).

Error Messages

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

This chapter lists the Cisco ONS 15454 error messages. Error message numbering is a new feature in Release 4.7. Table 3-1 gives a list of all error message numbers, the messages, and a brief description of each message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*).Error messages are an alert that an unexpected or undesirable operation has occurred which either indicates the risk of loss of traffic or an inability to properly manage devices in the network. Warnings are an alert that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

The error dialog box in Figure 3-1 consists of three parts: the error title (“Error”), the error ID (EID-2197), and the error message (“CORBA failure.Unable to proceed”).

Figure 3-1 Error Dialog Box

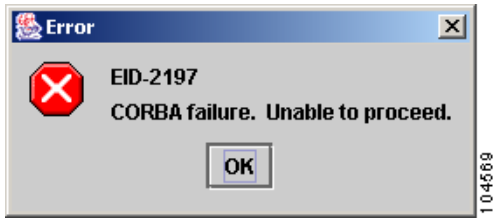


Table 3-1 Error Messages

Error ID	Error Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	Null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and re-start your browser in order for the new permissions to take effect.	Refer to error message text.
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	Refer to error message text.
EID-1003	An error was encountered while attempting to launch CTC. {0}	Unexpected exception/error while launching CTC from the applet. Failed to rollback card provisioning while cancelling a span upgrade. Unexpected error while assigning east or west protect port of a bidirectional line switched ring (BLSR).
EID-1004	Problem Deleting CTC Cache: {0} {1}	CTC encountered a problem deleting the cache.
EID-1005	An error occurred while writing to the {0} file.	CTC could not write the launching batch file.
EID-1006	The URL used to download {0} is malformed.	The URL used to download the Launcher.jar file is malformed.
EID-1007	An I/O error occurred while trying to download {0}.	An input/output exception was encountered when CTC tried to download the GUI launcher.
EID-1018	Password must contain at least 1 alphabetic, 1 numeric, and 1 special character (+, # or %). Password shall not contain the associated user-ID.	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename.	CTC could not create the file due to an invalid filename.
EID-1020	Fatal exception occurred, exiting CTC. Unable to switch to the Network view.	CTC was unable to switch from the node or card view to the network view, and is now shutting down.
EID-1021	Unable to navigate to {0}.	Failed to display the indicated view—node or network.
EID-1022	A session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to error message text.
EID-1023	This session has been terminated. This can happen if the card resets, the session has timed out, or if someone else (possibly using a different CTC) already has a session open with this slot.	Refer to error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-1026	Unable to locate HelpSet.	CTC was unable to locate the help set for the online help.
EID-1027	Unable to locate Help ID: {0}	CTC was unable to locate the help ID for the online help.
EID-1028	Error saving table. {0}	There was an error saving the specified table.
EID-1031	CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD.	Refer to error message text.
EID-1032	CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD.	Refer to error message text.
EID-1034	Unable to locate HelpSet when searching for Help ID "{0}".	CTC is unable to locate the subset {0} of the context sensitive help files.
EID-1035	CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required.	Refer to error message text.
WID-1036	WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner.	Refer to error message text.
EID-1037	Could not open {0}. Please enter another filename.	Refer to error message text.
EID-1038	The file {0} does not exist.	Refer to error message text.
EID-2001	No rolls selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The Roll must be completed or cancelled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	Error deleting roll.	There was an error when CTC tried to delete the roll.
EID-2004	No IOS slot selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files may have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.	CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.
EID-2006	Error editing circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	Unable to save preferences.	CTC cannot save the preferences.
EID-2008	Unable to store circuit preferences: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	Unable to download package: {0}	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2010	Delete destination failed.	CTC could not delete the destination.
EID-2011	Circuit destroy failed.	CTC could not destroy the circuit.
EID-2012	Reverse circuit destroy failed.	CTC could not reverse the circuit destroy.
EID-2013	Circuit creation error. Circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog will close. Please try again.	Refer to error message text.
EID-2014	No circuit(s) selected. {0}	You must select a circuit to complete this function.
EID-2015	Unable to delete circuit {0}as it has one or more rolls.	CTC cannot delete the circuit because it contains one or more rolls.
EID-2016	Unable to delete circuit.	There was an error deleting the circuit.
EID-2017	Error mapping circuit. {0}	There was an error mapping the circuit.
EID-2018	Circuit roll failure. The circuit has to be in the DISCOVERED state in order to perform a roll.	Refer to error message text.
EID-2019	Circuit roll failure. Current version of CTC does not support bridge and roll on a VT tunnel or VT aggregation point circuit.	Refer to error message text.
EID-2020	Circuit roll failure. The two circuits must have the same direction.	Refer to error message text.
EID-2021	Circuit roll failure. The two circuits must have the same size.	Refer to error message text.
EID-2022	Circuit roll failure. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to error message text.
EID-2023	Unable to create new user account.	Refer to error message text
EID-2024	Node selection error.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each of the endpoints of this circuit are running software that supports this feature.	Refer to error message text. This error is generated from the AnsOpticsParamsPane to indicate that the selected ring type is not supported by the endpoints of the circuit. In the VLAN pane it indicates that the back-end spanning tree protocol (STP) disabling is not supported.
EID-2026	Unable to apply UPSR request. {0}	Error occurred while attempting to switch a path protection circuit away from a span.
EID-2027	Error deleting circuit drop.	CTC could not delete the circuit drop.
EID-2028	Error removing circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.
EID-2030	Provisioning error.	There was an error during provisioning.
EID-2031	Error adding node.	There was an error while adding a node.
EID-2032	Unable to rename circuit. {0}	CTC could not rename the circuit.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2033	An error occurred during validation. {0}	There was an internal error while validating the user changes during Apply. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).
EID-2034	Unable to add network circuits: {0}	Refer to error message text.
EID-2035	The source and destination nodes are not connected.	Refer to error message text.
EID-2036	Cannot delete this {0}. LAN Access has been disabled on this node and this {0} is needed to access the node.	Refer to error message text.
EID-2037	Application error. Cannot find attribute for {0}.	CTC cannot find an attribute for the specified item.
EID-2038	Invalid protection operation.	There was an invalid protection operation.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	Refer to error message text.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to error message text.
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link.	Refer to error message text.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to error message text.
EID-2047	Error validating slot number. Please enter a valid value for the slot number.	Refer to error message text.
EID-2048	Error validating port number. Please enter a valid value for the port number.	Refer to error message text.
EID-2050	New circuit destroy failed.	CTC could not destroy the new circuit.
EID-2051	Circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.
EID-2052	Error during circuit processing.	There was an error during the circuit processing.
EID-2054	Endpoint selection error.	There was an error during the endpoint selection.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combo boxes.
EID-2056	Communication error. {0}	An internal error occurred while synchronizing alarms with the nodes. Network Alarm pane.
EID-2059	Node deletion Error. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	Error provisioning VLAN.	There was an error defining the VLAN.
EID-2062	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.
EID-2063	Cannot delete default VLAN.	The selected VLAN is the default VLAN, and cannot be deleted.
EID-2064	Error deleting VLANs. {0}	There was an error deleting the VLAN.
EID-2065	Cannot import profile. Profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.	Cannot import profile. The specified profile exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.
EID-2066	Unable to store profile. Error writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	File write error. {0}	CTC encountered a file write error.
EID-2068	Unable to load alarm profile from node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	File not found or I/O exception. {0}	Either the file was not found, or there was an input/output exception.
EID-2070	Failure deleting profile. {0}	The profile deletion failed.
EID-2071	Only one column may be highlighted.	Refer to error message text.
EID-2072	Only one profile may be highlighted.	Refer to error message text.
EID-2073	This column is permanent and may not be removed.	Refer to error message text.
EID-2074	Select one or more profiles.	Refer to error message text.
EID-2075	This column is permanent and may not be reset.	Refer to error message text.
EID-2077	This column is permanent and may not be renamed.	Refer to error message text.
EID-2078	At least two columns must be highlighted.	Refer to error message text.
EID-2079	Cannot load alarmables into table. There are no reachable nodes from which the list of alarmables may be loaded. Please wait until such a node is reachable and try again.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2080	Node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	Error removing profile {0} from node {1}.	There was an error removing the specified profile from the node.
EID-2082	Cannot find profile {0} on node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	Error adding profile {0} to node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	Invalid profile selection. No profiles were selected.	Refer to error message text.
EID-2086	Invalid node selection. No nodes were selected.	Refer to error message text.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to error message text.
EID-2088	Invalid profile name.	Refer to error message text.
EID-2089	Too many copies of {0} exist. Please choose another name.	Too many copies of the specified item exist.
EID-2090	No nodes selected. Please select the node(s) on which to store the profile(s).	Refer to error message text.
EID-2091	Unable to switch to node {0}.	CTC is unable to switch to the specified node.
EID-2092	General exception error.	CTC encountered a general exception error while trying to complete the task.
EID-2093	Not enough characters in name. {0}	There are not enough characters in the name.
EID-2094	Password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	Illegal password. {0}	The password you entered is not allowed.
EID-2096	The user must have a security level.	You must have an assigned security level to perform this task.
EID-2097	No user name specified.	You did not specify a user name.
EID-2099	Ring switching error.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	Refer to error message text.
EID-2101	Protection switching error.	There was an error during the protection switch.
EID-2102	The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	Error upgrading span.	There was an error during the span upgrade.
EID-2104	Unable to switch circuits back as one or both nodes are not reachable.	This error occurs during the path protection span upgrade procedure.
EID-2106	The node name cannot be empty.	You must supply a name for the node.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2107	Error adding {0}, unknown host.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item is already in the network.
EID-2109	The node is already in the current login group.	Refer to error message text.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Refer to error message text.
EID-2113	Cannot set extension byte for ring. {0}	CTC cannot set the extension byte.
EID-2114	Card communication failure. Error applying operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	Error applying operation. {0}	There was an error applying the specified operation.
EID-2116	Invalid extension byte setting. {0}	The extension byte set is invalid.
EID-2118	Cannot delete ring. There is a protection operation set. All protection operations must be clear for ring to be deleted.	Refer to error message text.
EID-2119	Cannot delete {0} because a protection switch is in effect. Please clear any protection operations, make sure that the reversion time is not "never" and allow any protection switches to clear before trying again.	Refer to error message text.
EID-2120	The following nodes could not be unprovisioned {0} Therefore you will need to delete this {1} again later.	The specified nodes could not be unprovisioned.
EID-2121	Cannot upgrade ring. {0}	CTC cannot upgrade the ring.
EID-2122	Inadequate ring speed for upgrade. Only {0} (or higher) {1} can be upgraded to 4-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber BLSR.
EID-2123	Verify that the following nodes have at least two in-service ports with the same speed as the 2-fiber {0}. The ports cannot serve as a timing reference, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two Unlocked-enabled ports with the same speed as the 2-fiber BLSR. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to error message text.
EID-2126	OSPF area error. {0}	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different STS regions on different spans. {0} Either select a different span or delete the above circuit(s).	Refer to error message text.
EID-2128	Illegal state error.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	This port is already assigned. The east and west ports must be different.	Refer to error message text.
EID-2130	The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999.	Refer to error message text.
EID-2131	Cannot set reversion to INCONSISTENT.	You must select another reversion type.
EID-2135	I/O error. Unable to store overhead circuit preferences. {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	Circuit merge error. {0}	There was an error merging the circuits.
EID-2138	Cannot delete all destinations. Please try again.	Refer to error message text.
EID-2139	Error updating destinations.	There was an error updating the circuit destinations.
EID-2143	No online help version selected. Cannot delete the online help book.	You cannot delete the online help.
EID-2144	Error deleting online help book(s). {0}	You cannot delete the online help.
EID-2145	Unable to locate a node with an IOS card.	Unable to locate a node with a Cisco IOS card.
EID-2146	Security violation. You may only logout your own account.	Refer to error message text.
EID-2147	Security violation. You may only change your own account.	Refer to error message text.
EID-2148	Security violation. You may not delete the account under which you are currently logged in.	Refer to error message text.
WID-2149	There is nothing exportable on this view.	Refer to error message text.
WID-2150	Node {0} is not initialized. Please wait and try again.	Refer to error message text.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to error message text.
WID-2153	Adding this drop makes the circuit a PCA circuit.	Refer to error message text.
WID-2154	Disallow creating monitor circuits on a port grouping circuit.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
WID-2155	Only partial switch count support on some nodes. {0}	Refer to error message text.
WID-2156	Manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error free.	Refer to error message text.
WID-2157	Cannot complete roll(s). {0}	CTC cannot complete the roll(s).
EID-2158	Invalid roll mode. {0}	The selected roll mode is invalid.
EID-2159	Roll not ready for completion. {0}	The roll is not ready for completion.
EID-2160	Roll not connected. {0}	The selected roll is not connected.
EID-2161	Sibling roll not complete. {0}	The sibling roll is not complete.
EID-2162	Error during roll acknowledgement. {0}	There was an error during the roll acknowledgement.
EID-2163	Cannot cancel roll. {0}	CTC cannot cancel the roll.
EID-2164	Roll error. {0}	CTC encountered a roll error.
WID-2165	The MAC address of node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	The MAC address of the specified node has been changed. All circuits originating from or dropping at this node need to be repaired.
WID-2166	Unable to insert node into the domain as the node is not initialized.	Refer to error message text.
WID-2167	Insufficient security privilege to perform this action.	You have insufficient security privilege to perform this action.
WID-2168	Warnings loading{0}. {1}	CTC encountered warnings while loading the specified item.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	Refer to error message text.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add profile. {1}	The profile list on the specified node is full. Please delete one or more profiles if you wish to add the specified profile.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to error message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The specified CTC CORBA (IIOP) listener port setting will be applied on the next CTC restart.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2173	Port unavailable. The desired CTC CORBA (IIOP) listener port, {0}, is already in use or you do not have permission to listen on it. Please select an alternate port.	The port is unavailable. The desired CTC Common Object Request Broker Architecture (CORBA) Internet Inter-ORB Protocol (IIOP) listener port is already in use or you do not have permission to listen on it. Please select an alternate port.
EID-2174	Invalid number entered. Please check it and try again.	You entered an invalid firewall port number.
WID-2175	Extension byte mismatch. {0}	There is a mismatch with the extension byte.
WID-2176	Not all spans have the same OSPF Area ID. This will cause problems with protection switching. To determine the OSPF Area for a given span, click on the span and the OSPF Area will be displayed in the pane to the left of the network map.	Refer to error message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to error message text.
WID-2179	There is no update as the circuit has been deleted.	Because the circuit has been deleted, there is no update for it.
EID-2180	CTC initialization failed in step {0}.	CTC initialization failed in the specified step.
EID-2181	This link may not be included as it originates from the destination.	Refer to error message text.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.
EID-2183	Circuit roll failure. Current version of CTC does not support bridge and roll on a VCAT circuit.	The value of the specified item is invalid.
EID-2184	Cannot enable the Spanning Tree Protocol on some ports because they have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign ethernet ports VLANs.	Refer to error message text.
EID-2185	Cannot assign the VLANs on some ports because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2186	Software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The maximum length for the ring name that can be used is {0}. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID within the specified range.
EID-2189	TL1 keyword "all" can not be used as the ring name. Please provide another name.	Refer to error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	Refer to error message text.
EID-2191	Ring name must not be empty.	You must supply a ring name.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2192	Cannot find a valid route for the circuit creation request.	Refer to error message text.
EID-2193	Cannot find a valid route for the circuit drop creation request.	Refer to error message text.
EID-2194	Cannot find a valid route for the roll creation request.	Refer to error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2196	Unable to relaunch the CTC. {0}	There is an error relaunching CTC.
EID-2197	CORBA failure. Unable to proceed. Please verify that the correct Java version is being used. Close and restart the CTC and browser applications.	There was a CORBA failure, and the task cannot proceed.
EID-2198	Unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified task.
EID-2200	CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one.	Refer to error message text.
EID-2202	Intra-node circuit must have two sources to be Dual Ring Interconnect.	Intra-node circuit must have two sources to be a dual-ring interconnect (DRI).
EID-2203	No member selected.	You must select a member.
EID-2204	Number of circuits must be a positive integer	The number of circuits cannot be negative.
EID-2205	Circuit Type must be selected	You must select a circuit type.
EID-2206	Unable to autoselect profile! Please select profile(s) to store and try again.	Refer to error message text.
EID-2207	You cannot add this span. Either the ring name is too big (i.e., ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	You cannot add this span. Either the ring name is too big (that is, the ring name length is greater than the specified length) or the endpoints do not support alphanumeric IDs.
EID-2208	This is an invalid or unsupported JRE.	The version of Java Runtime Environment (JRE) is either invalid or unsupported.
EID-2209	The user name must be at least {0} characters long.	The user name must be at least the specified character length.
EID-2210	No package name selected.	You must select a package name.
EID-2211	No node selected for upgrade.	You must select a node for the upgrade.
EID-2212	Protected Line is not provisionable.	The protected line cannot be provisioned.
W ID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The circuit state, specified by {0} cannot be applied to the selected drops.
EID-2214	The node is disconnected. Please wait till the node reconnects.	Refer to error message text.
EID-2215	Error while leaving {0} page.	There was an error while leaving the specified page.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-2216	Error while entering {0} page.	There was an error entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to error message text.
EID-2218	Bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	Protection operation failed, XC loopback is applied on cross-connection.	Protection operation failed; a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is PARTIAL. CTC will not be able to change it. Please try again later	Refer to error message text.
EID-2221	Cannot find a valid route for the unprotected to UPSR upgrade request.	Refer to error message text.
EID-2222	One or more of the following nodes are currently part of a 4-fiber {0}. Only a single 4-fiber {0} is supported per node. {1}	Refer to error message text.
EID-2223	Only one circuit can be upgraded at a time.	Refer to error message text.
EID-2224	This link may not be included as it terminates on the source.	Refer to error message text.
EID-2225	No valid signal while trying to complete the roll. (0)	Refer to error message text.
EID-2320	This VCAT circuit does not support deletion of its member circuits.	Refer to error message text.
EID-2321	Error deleting member circuits. {0}	Refer to error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They may appear as partial circuits.	Refer to error message text.
EID-2323	Circuit roll failure. Current version of CTC does not support bridge and roll on a DRI protected circuit.	Refer to error message text.
EID-2324	Circuit upgrade error. {0}	Refer to error message text.
EID-2325	You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box.	The maximum amount of attempts to unlock this session has been reached.
WID-2326	Current version of CTC does not support bridge and roll on circuits, which are entirely created by TL1. To continue with bridge and roll in CTC, selected circuits will be ungraded. CAUTION: Once circuits are upgraded, future bridge and roll on the circuits can only be done in CTC. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
WID-2327	Current version of CTC does not support bridge and roll on circuits, which are partially created by TL1. To continue with bridge and roll in CTC, selected circuits must be ungraded. CAUTION: Once circuits are upgraded, future bridge and roll on the circuits can only be done in CTC. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to error message text.
EID-2328	Circuit reconfigure error. {0}	Refer to error message text.
EID-2329	{0} of {1} circuits could not be successfully created.	Refer to error message text.
EID-2330	Circuit verification: selected {0} invalid! {1}	Refer to error message text.
EID-2331	Deleting {0} may be service affecting.	Refer to error message text.
EID-2332	Hold-off timer validation error in row [0]. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to error message text.
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	An Ethernet remote monitoring (RMON) threshold with the same parameters already exists. Please change one or more of the parameters and try again.
EID-3002	Error retrieving defaults from the node: {0}	There was an error retrieving the defaults from the specified node.
EID-3003	Cannot load file {0}.	CTC cannot load the specified file.
EID-3004	Cannot load properties from the node	Refer to error message text.
EID-3005	Cannot save NE Update values to file {0}	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	Cannot load NE Update properties from the node	Refer to error message text.
EID-3007	Provisioning Error for {0}	There was a provisioning error for the specified item.
EID-3008	Not a valid Card	You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Shelf view and try again.
EID-3009	No {0} selected	No item selected.
EID-3010	Unable to create bidirectional optical link	Refer to error message text.
EID-3011	The file {0} doesn't exist or cannot be read.	The specified file does not exist or cannot be read.
EID-3012	The size of {0} is zero.	The size of the item is zero.
EID-3013	{0} encountered while restoring database.	The specified item was encountered while restoring the database (DB).

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3014	Job terminated, {0} was encountered.	The job terminated because the specified item was encountered.
EID-3015	{0} encountered while performing DB backup.	The specified item was encountered while performing the DB backup.
EID-3016	Invalid subnet address.	Refer to error message text.
EID-3017	Subnet address already exists.	Refer to error message text.
EID-3018	Standby TSC not ready.	The standby Timing and Shelf Control card (TSC) not ready.
EID-3019	Incomplete internal subnet address.	There is an incomplete internal subnet address.
EID-3020	TSC One and TSC Two subnet addresses cannot be the same.	Refer to error message text.
EID-3021	An error was encountered while retrieving the diagnostics: {0}	CTC encountered an error.
EID-3022	Requested action not allowed.	The requested action is not allowed.
EID-3023	Unable to retrieve low order cross connect mode.	Refer to error message text.
EID-3024	Unable to switch low order cross connect mode.	Refer to error message text.
EID-3025	Error while retrieving thresholds.	The was an error retrieving the thresholds.
EID-3026	Cannot modify send DoNotUse.	CTC cannot modify Send DoNotUse.
EID-3027	Cannot modify SyncMsg.	CTC cannot modify SyncMsg.
EID-3028	Cannot change port type.	CTC cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port.	Refer to error message text.
EID-3031	Error hard-resetting card.	There was an error hard-resetting card.
EID-3032	Error resetting card.	There was an error resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to error message text.
EID-3035	The cross connect diagnostics cannot be performed	Refer to error message text.
EID-3036	The cross connect diagnostics test is not supported on this shelf.	The cross-connect diagnostics test is not supported on this shelf.
EID-3037	A software downgrade cannot be performed to the selected version while a SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	A software downgrade cannot be performed to the selected version while a Single-Shelf Cross-Connect (SSXC) card is inserted in this shelf. Please follow the steps to replace the SSXC with a Core Cross-Connect card (CXC) card before continuing the software downgrade.
EID-3038	A software downgrade cannot be performed at the present time.	Refer to error message text.
EID-3039	Card change error.	There was a card change error.
EID-3040	Invalid card type.	The card type is invalid.
EID-3041	Error applying changes.	There was an error applying the changes.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3042	The flow control low value must be less than the flow control high value for all ports in the card.	Refer to error message text.
EID-3043	Error while retrieving line info settings.	Refer to error message text.
EID-3044	Error while retrieving line admin info settings.	Refer to error message text.
EID-3045	Error while retrieving transponder line admin info settings.	Refer to error message text.
EID-3046	The flow control water mark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the specified values.
EID-3047	The file named {0} could not be read. Please check the name and try again.	The specified file could not be read. Please check the name and try again.
EID-3048	There is no IOS startup config file available to download.	There is no Cisco IOS startup configuration file available to download.
EID-3049	There is an update in progress so the download cannot be done at this time.	Refer to error message text.
EID-3050	An exception was caught trying to save the file to your local file system.	Refer to error message text.
EID-3051	The maximum size for a config file in bytes is: {0}	The maximum size for a configuration file in bytes is the value specified in the message.
EID-3052	There was an error saving the config file to the TCC.	Refer to error message text.
EID-3053	The value of {0} must be between {1} and {2}	The value of the item must be between the specified values.
EID-3054	Cannot remove provisioned input/output ports or another user is updating the card, please try later.	Cannot remove provisioned input/output ports or another user is updating the card. Please try later.
EID-3055	Cannot create soak maintance pane.	CTC cannot create Soak Maintenance Pane.
EID-3056	Cannot save defaults to file {0}	Cannot save defaults to the specified file.
EID-3057	Cannot load default properties from the node.	Refer to error message text.
EID-3058	File {0} does not exist.	The specified file does not exist.
EID-3059	Error encountered while refreshing.	There was an error in refreshing.
EID-3060	The ALS Recovery Pulse Interval must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between 100 seconds and 300 seconds.
EID-3061	The ALS Recovery Pulse Duration must be between {0} seconds and {1} seconds.	The ALS Recovery Pulse Width must be between 2.00 seconds and 100.0 seconds.
EID-3062	Error encountered while setting values.	Refer to error message text.
EID-3063	Unable to retriever bridge port settings.	Refer to error message text.
EID-3064	Not a G1000 Card.	This card is not a G1000 card.
EID-3065	An error was encountered while attempting to create RMON threshold: {0}	You must create an RMON threshold.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3066	Minimum sample period must be greater than or equal to 10.	Refer to error message text.
EID-3067	Rising Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	Falling Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.
EID-3069	Rising threshold must be greater than or equal to falling threshold.	Refer to error message text.
EID-3070	Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied.	There was an error in the data for the specified ports. Exactly one VLAN must be marked Untagged for each port. These changes will not be applied.
EID-3071	Get Learned Address	Unable to retrieve the learned MAC address from the NE.
EID-3072	Clear Learned Address	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	Clear Selected Rows	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3074	Clear By {0}	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in param column needs to be selected.	Refer to error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to error message text.
EID-3077	No optical link selected.	Refer to error message text.
EID-3078	Unable to create optical link.	Refer to error message text.
EID-3079	Cannot apply defaults to node: {0}	Cannot apply defaults to the specified node.
EID-3080	Cannot go to the target tab {0}	Cannot go to the target tab.
EID-3081	Port type can't be changed.	Refer to error message text.
EID-3082	Cannot modify the {0} extension byte.	Cannot modify the extension byte.
EID-3083	Error while retrieving stats.	Error in getting statistics.
EID-3084	Error encountered while trying to retrieve laser parameters for {0}	
EID-3085	No OSC Terminations selected	Refer to error message text.
EID-3086	One or more Osc terminations could not be created.	Refer to error message text.
EID-3087	OSC termination could not be edited.	Refer to error message text.
EID-3088	No {0} card to switch.	No card of the specified type to switch.
EID-3089	Cannot use/change {0} state when {1} is failed or missing.	Cannot use/change the specified state when it is failed or missing.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3090	Cannot perform operation as {0} is {1}LOCKED_ON/LOCKED_OUT.	Cannot perform operation.
EID-3091	Cannot perform the operation as protect is active.	Refer to error message text.
EID-3092	Invalid service state. The requested action cannot be applied.	Refer to error message text.
EID-3093	Cannot perform the operation as duplex pair is {0}locked.	Refer to error message text.
EID-3094	Cannot perform the operation as no XC redundancy is available.	Refer to error message text.
EID-3095	Deletion failed since the circuit is in use	Refer to error message text.
WID-3096	Internal communication error encountered while trying to retrieve laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again.	Refer to error message text.
EID-3097	The ring termination is in use.	Refer to error message text.
EID-3098	No ring terminations selected.	Refer to error message text.
EID-3099	Sorry, entered key does not match existing authentication key.	The entered key does not match existing authentication key.
EID-3100	Error encountered during authentication.	There was an error in authentication.
EID-3101	DCC Metric is not in the range 1 - 65535.	The DCC Metric is not in the range 1 to 65535.
EID-3102	Invalid DCC Metric	There was an Invalid DCC Metric.
EID-3103	Invalid IP Address: {0}	The IP Address is Invalid.
EID-3104	Router priority is not in the range of 0 - 255	The Router priority is not in the range of 0 to 255.
EID-3105	Invalid Router Priority	The Router Priority is Invalid.
EID-3106	Hello Interval is not in the range of 1 - 65535	The Hello Interval is not in the range of 1 to 65535.
EID-3107	Invalid Hello Interval	The Hello Interval is Invalid.
EID-3109	Invalid Dead Interval value. Valid range is 1 - 2147483647	The Dead Interval is invalid.
EID-3110	Dead Interval must be larger than Hello Interval	Refer to error message text.
EID-3111	LAN transit delay is not in the range of 1 - 3600 seconds	The LAN transit delay is not in the range of 1 to 3600 seconds.
EID-3112	Invalid Transmit Delay	The transmit delay is invalid.
EID-3113	Retransmit Interval is not in the range 1 - 3600 seconds	The retransmit interval is not in the range 1 to 3600 seconds.
EID-3114	Invalid Retransit Interval	The retransmit interval is invalid.
EID-3115	LAN Metric is not in the range 1 - 65535.	The LAN Metric is not in the range 1 to 65535.
EID-3116	Invalid LAN Metric	The LAN Metric is invalid.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3117	If OSPF is active on LAN, no DCC Area Ids may be 0.0.0.0. Please change all DCC Area Ids to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to error message text.
EID-3118	If OSPF is active on LAN, LAN Area ID may not be the same as DCC Area Id.	Refer to error message text.
EID-3119	Validation Error	The Cisco Transport Controller (CTC) was unable to validate the values entered by the user. This error message is common to several different provisioning panes within CTC (examples include the SNMP provisioning pane, the Genera l> Network provisioning pane, the Security > Configuration provisioning pane, etc.).
EID-3120	No object of type {0} selected to delete.	No object of the selected type selected to delete.
EID-3121	Error Deleting {0}	There is an error deleting the item.
EID-3122	No object of type {0} selected to edit.	No object of the specified type selected to edit.
EID-3123	Error Editing {0}	There was an error editing the item.
EID-3124	{0} termination is in use. Check if {0} is used by IPCC.	The specified termination is in use.
EID-3125	No {0} Terminations selected.	No specified terminations are selected.
EID-3126	{0} termination could not be edited.	The specified termination could not be edited.
EID-3127	Unable to provision orderwire because E2 byte is in use by {0}.	Refer to error message text.
EID-3128	The authentication key may only be {0} characters maximum	The authentication key can only be the specified characters maximum.
EID-3129	The authentication keys do not match!	Refer to error message text.
EID-3130	Error creating OSPF area virtual link.	CTC encountered an error creating the Area Virtual Link.
EID-3131	Error creating OSPF virtual link.	CTC encountered an error creating the Virtual Link.
EID-3132	Error setting OSPF area range: {0}, {1}, false.	CTC encountered an error setting the area range for the specified values.
EID-3133	Max number of OSPF area ranges exceeded.	The maximum number of area ranges has been exceeded.
EID-3134	Invalid Area ID. Use DCC OSPF Area ID, LAN Port Area ID, or 0.0.0.0.	Refer to error message text.
EID-3135	Invalid Mask	Refer to error message text.
EID-3136	Invalid Range Address	Refer to error message text.
EID-3137	Your request has been rejected because the timing source information was updated while your changes were still pending. Please retry.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3138	Invalid clock source for switching.	Refer to error message text.
EID-3139	Cannot switch to a reference of inferior quality.	Refer to error message text.
EID-3140	Higher priority switch already active.	Refer to error message text.
EID-3141	Attempt to access a bad reference.	Refer to error message text.
EID-3142	No Switch Active.	Refer to error message text.
EID-3143	Error creating static route entry.	Refer to error message text.
EID-3144	Max number of static routes exceeded.	The maximum number of static routes has been exceeded.
EID-3145	RIP Metric is not in the range 1-15.	The Routing Information Protocol (RIP) metric is not in the range 1 to 15.
EID-3146	Invalid RIP Metric	Refer to error message text.
EID-3147	Error creating summary address.	Refer to error message text.
EID-3148	No Layer 2 domain has been provisioned.	Refer to error message text.
EID-3149	Unable to retrieve MAC addresses.	Refer to error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writeable.	The specified target file is not writeable.
EID-3152	Error creating Protection Group	CTC encountered an error creating Protection Group.
EID-3153	Cannot delete card, it is in use.	Cannot delete card. It is in use.
EID-3154	Cannot {0} card, provisioning error.	CTC cannot perform the task on the card.
EID-3155	Error Building Menu	CTC encountered an error building the menu.
EID-3156	Error on building menu (cards not found for {0} group)	CTC encountered an error on building menu (cards not found for the specified group).
EID-3157	Unable to set selected model: unexpected model class {0}	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Unable to switch, a similar or higher priority condition exists on peer or far-end card.	Refer to error message text.
EID-3159	Error applying operation.	CTC encountered an error applying this operation.
EID-3160	{0} error encountered.	CTC encountered the displayed error.
EID-3161	Ring Upgrade Error	An error was encountered while attempting to upgrade the BLSR or MS-SPRing. Refer to the details portion of the error dialog box for more information.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to error message text.
EID-3163	Cannot validate data for row {0}	Cannot validate data for the specified row.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3164	New Node ID ({0}) for Ring ID {1} duplicates ID of node {2}	The new specified Node ID for the specified Ring ID is the same as the second specified Node ID.
EID-3165	The Ring ID provided is already in use. Ring IDs must be unique	Refer to error message text.
EID-3166	Error refreshing {0} table	CTC encountered an error refreshing the specified table.
EID-3167	Slot already in use	Refer to error message text.
EID-3168	Provisioning Error	An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information.
EID-3169	Error Adding Card	CTC encountered an error adding the card.
EID-3170	Cannot delete card, {0}	Cannot delete the specified card.
EID-3171	Error creating Trap Destination	CTC encountered an error creating the trap destination.
EID-3172	No RMON Thresholds selected	Refer to error message text.
EID-3173	The contact "{0}" exceeds the limit of {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The location "{0}" exceeds the limit of {1} characters.	The specified location exceeds the specified character limit.
EID-3175	The operator identifier "{0}" exceeds the limit of {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information "{0}" exceeds the limit of {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The node name cannot be empty.	The specified name is empty.
EID-3178	The name "{0}" exceeds the limit of {1} characters.	The specified name exceeds the specified character limit.
EID-3179	Protect card is in use.	Refer to error message text.
EID-3180	1+1 Protection Group does not exist.	Refer to error message text.
EID-3181	Y Cable Protection Group does not exist.	Refer to error message text.
EID-3182	The Topology Element is in use and cannot be deleted as requested	Refer to error message text.
EID-3183	Error Deleting Protection Group	CTC encountered an error deleting the protection group.
EID-3184	No {0} selected.	You must select an item before completing this task.
EID-3185	There is a protection switch operation on this ring. Therefore, it cannot be deleted at this time.	Refer to error message text.
EID-3186	Busy {0} is {1} and cannot be deleted as requested.	The item is in use and cannot be deleted as requested.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3187	Error deleting trap destination.	CTC encountered an error deleting the trap destination.
EID-3214	Could not get number of HOs for line.	Refer to error message text.
EID-3215	Error in refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	Invalid proxy port.	Invalid Proxy port.
EID-3217	Could not refresh stats.	Could not refresh statistics.
EID-3218	Unable to launch automatic node setup.	Refer to error message text.
EID-3219	Unable to refresh automatic node setup information.	Failure trying to retrieve optical link information.
EID-3220	Error refreshing row {0}	Error refreshing the specified row.
EID-3222	Could not clear stats.	Refer to error message text.
EID-3223	Error cancelling software upgrade.	Refer to error message text.
EID-3224	Error accepting load.	Refer to error message text.
EID-3225	Error while refreshing pane.	Refer to error message text.
EID-3226	{0} termination(s) could not be deleted. {1}	Refer to error message text.
EID-3227	Unable to record a baseline, performance metrics will remain unchanged.	Refer to error message text.
EID-3228	{0} termination(s) could not be created. {1}	Refer to error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	RIP is active on the LAN. Please disable RIP before enabling OSPF.
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	OSPF is active on the LAN. Please disable OSPF before enabling RIP.
EID-3231	Error in Set OPR	An error was encountered while attempting to provision the Optical Power Received (OPR).
EID-3232	Cannot transition port state indirectly: try editing directly	Refer to error message text.
EID-3233	Current loopback provisioning does not allow this state transition	Refer to error message text.
EID-3234	Current synchronization provisioning does not allow this state transition	Refer to error message text.
EID-3235	Cannot perform requested state transition on this software version.	Refer to error message text.
EID-3236	Database Restore failed. {0}	The specified database restore failed.
EID-3237	Database Backup failed. {0}	The specified database backup failed.
EID-3238	Send PDIP setting on {0} is inconsistent with that of control node {1}	Send payload defect indication (PDIP) setting on the specified item is inconsistent with that of the specified control node.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3239	The overhead termination is invalid	Refer to error message text.
EID-3240	The maximum number of overhead terminations has been exceeded.	Refer to error message text.
EID-3241	The {0} termination port is in use.	The specified termination port is in use.
EID-3242	LDCC exists on the selected ports. Please create SDCC one by one.	The line DCC (LDCC) exists on the selected ports. Please create SDCC one by one.
WID-3243	LDCC exists on the selected port. Please remove one after the connection is created.	An LDCC exists on this port. Delete the LDCC after the connection is created.
EID-3244	SDCC exists on the selected ports. Please create LDCC one by one.	SDCC exists on the selected ports. Please create LDCC one by one.
WID-3245	SDCC exists on the selected port. Please remove one after the connection is created.	An SDCC exists on this port. Delete the SDCC after the connection is created.
EID-3246	Wizard unable to validate data: {0}	CTC encountered an error.
EID-3247	Ordering error. The absolute value should be {0}	Ordering error. The absolute value should be the number specified.
EID-3248	Wrong parameter is changed: {0}	CTC changed the wrong parameter.
EID-3249	Invalid voltage increment value.	Refer to error message text.
EID-3250	Invalid power monitor range.	Refer to error message text.
EID-3251	Unable to complete requested action. {0}	CTC is unable to complete requested action.
EID-3252	No download has been initiated from this CTC session.	Refer to error message text.
EID-3253	Reboot operation failed. {0}	The reboot operation failed.
EID-3254	Validation Error. {0}	The Cisco Transport Controller (CTC) was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning panes within the CTC.
EID-3255	Can not change timing configuration, manual/force operation is performed.	Refer to error message text.
WID-3256	Could not assign timing reference(s) because - at least one timing reference has already been used and/or - a timing reference has been attempted to be used twice. Please use the “Reset” button and verify the settings.	Refer to error message text.
EID-3257	Duplicate DCC number detected: {0}.	CTC detected a duplicate DCC number.
EID-3258	There was a software error attempting to download the file. Please try again later.	Refer to error message text.
EID-3259	Create FC-MR Threshold	You must create an FCMR threshold.
EID-3260	An error was encountered while provisioning the internal subnet: {0}	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	Refer to error message text.
EID-3262	The port provisioning cannot be changed when the port status is not OOS.	Refer to error message text.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded.
EID-3264	The port provisioning cannot be changed while the port is in service.	Refer to error message text.
EID-3265	Error modifying Protection Group	There was an error modifying the protection group.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to error message text.
WID-3267	Cannot edit XTC protection group.	Refer to error message text.
WID-3268	Invalid entry. {0}	The entry is invalid.
WID-3269	{0} was successfully initiated for {1} but its completion status was not able to be obtained from the node. {0} may or may not have succeeded. When the node is accessible, check its software version.	The specified task was successfully initiated for the item, but its completion status was not able to be obtained from the node. The task might or might not have succeeded. When the node is accessible, check its software version.
WID-3270	The file {0} does not exist.	The specified file does not exist.
WID-3271	The value entered must be greater than {0}.	The value entered must be greater than the value shown.
WID-3272	Entry required	An entry is required for this task.
WID-3273	{0} already exists in the list.	The specified item already exists in the list.
WID-3274	A software upgrade is in progress. Network configuration changes that results a node reboot can not take place during software upgrade. Please try again after software upgrade is done.	Refer to error message text.
WID-3275	Make sure the Remote Interface ID and the Local Interface ID on the two sides are matched. (Local Interface ID on this node should equal Remote Interface ID on the neighbor node and vice-versa.)	The specified item already exists in the list.
WID-3276	Both SDCC and LDCC exist on the same selected port. {0}	Refer to error message text.
WID-3277	The description cannot contain more than {0} characters. Your input will be truncated.	Refer to error message text.
WID-3279	Card deleted, returning to shelf view.	Refer to error message text.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
WID-3281	A software upgrade is in progress. {0} can not proceed during a software upgrade. Please try again after the software upgrade has completed.	Refer to error message text.
WID-3282	Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following 15600s are currently unsafe to upgrade...	Refer to error message text. Specific to the 15600 only.
WID-3283	There is a protection switch or another protection operation applied on the ring. Applying this protection operation now will probably cause a traffic outage. OK to continue?	Refer to error message text.
WID-3284	Protection Channel Access circuit found on {0} being set to non-revertive. These circuits will not be able to re-establish after ring or span switch. OK to continue?	Refer to error message text.
WID-3285	Applying FORCE or LOCKOUT operations may result in traffic loss.	Refer to error message text.
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to error message text.
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to error message text.
WID-3288	This ring status is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Refer to error message text.
EID-3290	Unable to delete specified provisionable patchcord(s).	Refer to error message text.
EID-3291	Cannot change revertive behavior due to an active protection switch.	Refer to error message text.
EID-3292	Error resetting shelf.	Refer to error message text.
EID-3293	No such provisionable patchcord.	You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently.
EID-3294	No RMON thresholds available for selected port.	Refer to error message text.
EID-3295	This card does not support RMON thresholds.	Refer to error message text.
EID-3296	Buffer-to-buffer credit is only supported for FC and FICON.	Refer to error message text.
EID-3298	ALS Auto Restart is not supported by this interface.	Refer to error message text.
EID-3300	Can not have duplicate OSPF Area IDs.	Refer to error message text.
EID-3301	LAN metric may not be zero.	Refer to error message text.
EID-3302	Standby {0} not ready.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3303	DCC Area ID and {0} conflict. {1}	Refer to error message text.
EID-3304	DCC number is out of range.	Refer to error message text.
EID-3305	Can not have OSPF turned on the LAN interface and the back bone area set on a DCC interface.	Refer to error message text.
EID-3306	Ethernet circuits must be bidirectional.	Refer to error message text.
EID-3307	Error while creating connection object at {0}.	Refer to error message text.
EID-3308	DWDM Link can be used only for optical channel circuits.	Refer to error message text.
EID-3309	OCH-NC circuit: link excluded - wrong direction.	Refer to error message text.
EID-3310	DWDM Link does not have wavelength available.	Refer to error message text.
EID-3311	Laser already on.	Refer to error message text.
EID-3312	Unable to change the power setpoint {0} {1}	Refer to error message text.
EID-3313	Unable to modify offset. Amplifier port is in service state.	Refer to error message text.
EID-3314	Requested action not allowed. Invalid state value.	Refer to error message text.
EID-3315	Unable to perform operation.	CTC is unable to perform operation.
EID-3316	Wrong node side.	This task was applied to the wrong node side.
EID-3317	Name too long.	The name you entered is too long.
EID-3318	Illegal name.	The name you entered is illegal.
EID-3319	Wrong line selection.	You selected the wrong line.
EID-3320	Unable to delete optical link.	CTC is unable to delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to error message text.
EID-3322	Equipment is not plugged-in.	At least one equipment is not plugged in.
EID-3323	APC system is busy.	Automatic Power Control (APC) system is busy.
EID-3324	No path to regulate.	There is no circuit path to be regulated.
EID-3325	Requested action not allowed.	Generic DWDM provisioning failure message.
EID-3326	Wrong input value.	The input value is incorrect.
EID-3327	Error in getting thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.
EID-3328	Error applying changes to row {0}.Value out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to error message text.
EID-3331	Error applying changes to row.	There was an error applying changes to the row.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3334	Cannot change timing parameters on protect port.	You cannot change timing parameters on protect port.
EID-3335	This port's type cannot be changed: SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	This port's type cannot be changed. The SDH validation check failed. Check to see if this port is part of a circuit, protection group, SONET DCC, orderwire, or User Network Interface, client (UNI-C) interface.
EID-3336	Error on reading a control mode value.	The Control Mode must be retrieved.
EID-3337	Error on setting a set point gain value.	The Gain Set Point must be set.
EID-3338	Error on reading a set-point gain value.	The Gain Set Point must be retrieved.
EID-3339	Error on setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	Error on setting expected wavelength.	The expected wavelength must be set.
EID-3341	Error on reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	Error on reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	Error on reading actual band.	The actual band must be retrieved.
EID-3344	Error on reading expected band.	The expected band must be retrieved.
EID-3345	Error on setting expected band.	The expected band must be set.
EID-3346	Error retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	Cannot load file {0}.	CTC cannot load the specified file.
EID-3348	Cannot load properties from the node.	CTC cannot load properties from the node.
EID-3349	Cannot save NE Update values to file.	CTC cannot save NE Update values to file.
EID-3350	Cannot load NE Update properties from the node:	CTC cannot load NE Update properties from the node.
EID-3351	File {0} does not exist.	The specified file does not exist.
EID-3352	Error on setting value at {0}.	There was an error setting the value at the specified location.
EID-3353	There is no such interface available.	No such interface exists in CTC.
EID-3354	Specified endpoint is in use.	The end point is in use.
EID-3355	Specified endpoint is incompatible.	The end point is incompatible.
EID-3357	Unable to calculate connections.	CTC is unable to calculate connections.
EID-3358	Optical link model does not exist for specified interface.	The OptLinkModel does not exist for the specified index.
EID-3359	Unable to set optical parameters for the node.	Refer to error message text.
EID-3361	Ring termination is in use. Error deleting ring termination	Refer to error message text.
EID-3362	Error deleting ring termination.	There was an error deleting ring termination.
EID-3363	No ring terminations selected.	You must select a ring termination.
EID-3364	Error creating ring ID.	There was an error creating the ring ID.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-3365	OSC termination is in use.	The OSC termination is in use.
EID-3366	Error deleting OSC termination.	There was an error deleting the OSC termination.
EID-3370	No optical link has been selected	You must select an optical link.
EID-3371	Error while calculating automatic optical link list.	There was an error calculating the automatic optical link list.
EID-3372	Attempt to access an OCH-NC connection that has been destroyed.	Refer to message text.
EID-3375	Expected span loss must be set.	Refer to error message text.
EID-3376	Unable to retrieve measured span loss.	Refer to error message text.
EID-3377	Wrong interface used.	Refer to error message text.
EID-3378	Duplicate origination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node.
EID-3379	Duplicate termination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node.
EID-3380	Unable to locate host.	Refer to error message text.
EID-3381	Maximum Frame size must be between {0} and {1} and may be increased in increments of {2}.	Refer to error message text.
EID-3382	Number of credits must be between {0} and {1}.	Refer to error message text.
EID-3383	GFP Buffers Available must be between {0} and {1} and may be increased in increments of {2}.	Refer to error message text.
WID-3384	You are about to force the use of Secure Mode for this chassis. You will not be able to undo this operation. OK to continue?	Refer to error message text.
EID-3385	{0}. Delete circuits, then try again.	Refer to error message text.
EID-3386	Unable to provision transponder mode: {0}	Refer to error message text.
EID-3387	You must change port{0} to an out-of-service state before changing card parameters. Click Reset to revert the changes.	Refer to error message text.
EID-3388	Unable to change the card mode because the card has circuits.	Refer to error message text.
EID-3389	Error encountered while changing the card mode.	Refer to error message text.
EID-3390	Port is in use.	Refer to error message text.
EID-3391	Unable to change the port rate because the port has been deleted.	Refer to error message text.
WID-3392	Could not assign timing reference(s) because - with external timing, only a single protected, or two unprotected timing references per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
WID-3393	Could not assign timing reference(s) because - with line or mixed timing, only a single unprotected timing reference per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to error message text.
WID-3394	Error refreshing Power Monitoring values.	Refer to error message text.
WID-3395	Invalid IP Configuration: {0}	Error in IP address, net mask length, default router, or a restricted IIOP port was selected.
EID-3396	Invalid Configuration: The standby controller card is not a TCC2P card.	Refer to error message text.
EID-3397	Wrong version for file {0}.	Refer to error message text.
EID-3398	Cannot delete PPM.	Refer to error message text.
EID-3399	Cannot delete PPM. It has port(s) in use.	Refer to error message text.
EID-3400	Unable to switch, force to Primary Facility not allowed.	Refer to error message text.
EID-3401	{0} cannot be provisioned for the port while {1} is enabled.	The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other.
EID-3402	Unable to complete the FORCE operation. The protect card is either not present or is not responding. Please check the protect card state and try again.	Refer to error message text.
EID-3403	Cannot perform requested state transition on monitored port.	Refer to error message text.
EID-3404	The far end IP address could not be set on the {0} termination. The IP address cannot be: loopback (127.0.0.0/8) class D (224.0.0.0/4) class E (240.0.0.0/4) broadcast (255.255.255.255/32) internal {1}	Refer to error message text.
EID-4000	The {0} ring name cannot be changed now. A {0} switch is active.	Refer to error message text.
EID-4001	The {0} ring ID cannot be changed now. A {0} switch is active.	Refer to error message text.
EID-5000	Cannot find a valid route for tunnel change request.	Refer to error message text.
EID-5001	Tunnel could not be changed.	Refer to error message text.
EID-5002	Tunnel could not be restored and must be recreated manually.	Refer to error message text.
EID-5003	Circuit roll failure. {0}	Refer to error message text.
EID-5004	There is already one 4F {0} provisioned on the set of nodes involved in {1}. The maximum number of 4F {0} rings has been reached for that node.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
WID-5005	A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors.	Refer to error message text.
WID-5006	Warning: Different secondary {0} node should only be used for DRI or Open-ended path protected circuits.	Refer to error message text.
WID-5007	If you change the scope of this view, the contents of this profile editor will be lost.	Refer to error message text.
WID-5008	Please make sure all the protection groups are in proper state after the cancellation.	Refer to error message text.
WID-5009	Circuit {0} not upgradable. No {1} capable {2}s are available at node {3}.	Refer to error message text.
EID-5010	Domain name already exists.	Refer to error message text.
EID-5011	Domain name may not exceed {0} characters.	Refer to error message text.
WID-5012	Software load on {0} does not support the addition of a node to a 1+1protection group.	Refer to error message text.
EID-5013	{0} doesn't support Bridge and Roll Feature. Please select a different port.	Refer to error message text.
EID-5014	An automatic network layout is already in progress, please wait for it to complete for running it again.	Refer to error message text.
WID-5015	{0} cannot be applied to {1}.	Refer to error message text.
EID-5016	An error was encountered while attempting to provision the {0}. {1}	Refer to error message text.
EID-5017	Unable to rollback provisioning, the {0} may be left in an INCOMPLETE state and should be manually removed.	Refer to error message text.
EID-6000	Platform does not support power monitoring thresholds	Refer to error message text.
EID-6001	One of the XC cards has failures or is missing.	Refer to error message text.
EID-6002	One of the XC cards is locked.	Refer to error message text.
EID-6003	Unable to create OSC termination. Ring ID already assigned.	Refer to error message text.
EID-6004	Unable to perform a system reset while a BLSR ring is provisioned on the node.	Refer to error message text.
EID-6005	Could not assign timing references: - Only two DS1 or BITS interfaces can be specified. - DS1 interfaces cannot be retimed and used as a reference - BITS-2 is not supported on this platform.	Refer to error message text.
EID-6006	Could not assign timing references: - NE reference can only be used if timing mode is LINE. - A BITS reference can only be used if timing mode is not LINE. - A line reference can only be used if timing mode is not EXTERNAL.	Refer to error message text.

Table 3-1 Error Messages (continued)

Error ID	Error Message	Description
EID-6007	Cancelling a software upgrade during standby TSC clock acquisition may result in a traffic outage.	Refer to error message text.
WID-6007	Cancelling a software upgrade during standby TSC clock acquisition may result in a traffic outage	Refer to error message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	Refer to error message text.
WID-6009	If Autoadjust GFP Buffers is disabled, GFP Buffers Available must be set to an appropriate value based on the distance between the circuit end points.	Refer to error message text.
WID-6010	If Auto Detection of credits is disabled, Credits Available must be set to a value less than or equal to the number of receive credits on the connected FC end point.	Refer to error message text.
WID-6011	Idle filtering should be turned off only when required to operate with non-Cisco FibreChannel/FICON-over-SONET equipment.	Refer to error message text.
EID-6012	Could not change the retiming configuration. There are circuits on this port	Refer to error message text.
EID-6013	NTP/SNTP server could not be changed. {1}	Refer to error message text.
EID-6014	Operation failed. The reference state is OOS.	Refer to error message text.
EID-6015	Distance Extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6016	Card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6017	The destination of a static route cannot be a node IP address.	Refer to error message text.
EID-6018	The destination of a static route cannot be the same as the subnet used by the node.	Refer to error message text.
EID-6019	The destination of a static route cannot be 255.255.255.255	Refer to error message text.
EID-6020	The destination of a static route cannot be the loopback network (127.0.0.0/8)	Refer to error message text.
EID-6021	The subnet mask length for a non-default route must be between 8 and 32.	Refer to error message text.
EID-6022	The subnet mask length for a default route must be 0.	Refer to error message text.

CHAPTER 4

Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, and set thresholds, and to report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for electrical cards, Ethernet cards, optical cards, and dense wavelength division multiplexing (DWDM) cards in the Cisco ONS 15454.

Note Release 4.7 is DWDM only. It supports all DWDM, transponder (TXP), and muxponder (MXP) cards but not optical, electrical, storage media access, or Ethernet cards. DWDM cards include the OSCM, OSC-CSM,OPT-PRE,OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.xAD-4B-xx.x, AD-1B-xx.x, AD-4C-xx.x, AD-2C-xx.x, AD-1C-xx.x, and the 32WSS

For information about enabling and viewing PM values, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Chapter topics include:

Note For additional information regarding PM parameters, refer to Telcordia documents GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE and the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

4.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter. You can set individual PM threshold values from the Cisco Transport Controller (CTC) card view Provisioning tab. For procedures on provisioning card thresholds, such as line, path, and SONET thresholds, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and displayed by CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If zero is entered as the threshold value, generation of TCAs is disabled but performance monitoring continues.

Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical DS-1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

4.2 Intermediate Path Performance Monitoring

Intermediate path performance monitoring (IPPM) allows transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. Many large networks only use line terminating equipment (LTE), not path terminating equipment (PTE). Table 4-1 shows ONS 15454 cards that are considered LTE.

Table 4-1 ONS 15454 Line Terminating Equipment

Electrical LTE	
ONS 15454 EC1-12	
ONS 15454 Optical LTE	
OC3 IR 4/STM1 SH 1310	OC3 IR/STM1 SH 1310-8
OC12 IR/STM4 SH1310	OC12 LR/STM4 LH1310
OC12 LR/STM4 LH 1550	OC12 IR/STM4 SH 1310-4
OC48 IR 1310	OC48 LR 1550
OC48 IR/STM16 SH AS 1310	OC48 LR/STM16 LH AS 1550
OC48 ELR/STM16 EH 100 GHz	OC48 ELR 200 GHz
OC192 SR/STM64 IO 1310	OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550	OC192 LR/STM64 LH ITU 15xx.xx
TXP_MR_10G	MXP_2.5G_10G
MXP_MR_2.5G	MXPP_MR_2.5G

ONS 15454 Software R3.0 and higher allows LTE cards to monitor near-end PM data on individual STS payloads by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor large amounts of STS traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on STS paths that have IPPM enabled, and TCAs are raised only for PM parameters on the IPPM enabled paths. The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P.

Note Far-end IPPM is not supported by all OC-N cards. It is supported by OC3-4 and EC-1 cards. However, SONET path PMs can be monitored by logging into the far-end node directly.

The ONS 15454 performs IPPM by examining the overhead in the monitored path and by reading all of the near-end path PM values in the incoming direction of transmission. The IPPM process allows the path signal to pass bidirectionally through the node completely unaltered.

For detailed information about specific IPPM parameters, locate the card name in the following sections and review the appropriate definition.

4.3 Pointer Justification Count Performance Monitoring

Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks. When a network is out of sync, jitter and wander occur on the transported signal. Excessive wander can cause terminating equipment to slip.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key causing data to be transmitted again.

Pointers provide a way to align the phase variations in STS and VT payloads. The STS payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the STS synchronous payload envelope (SPE) called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-PDet-P) or path-generated (PPJC-PGen-P) positive pointer justifications. NPJC is a count of path-detected (NPJC-PDet-P) or path-generated (NPJC-PGen-P) negative pointer justifications depending on the specific PM name. PJCDIFF is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. PJCS-PDet-P is a count of the one-second intervals containing one or more PPJC-PDet or NPJC-PDet. PJCS-PGen-P is a count of the one-second intervals containing one or more PPJC-PGen or NPJC-PGen.

A consistent pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. Positive pointer adjustments occur when the frame rate of the SPE is too slow in relation to the rate of the STS 1.

You must enable PPJC and NPJC performance monitoring parameters for LTE cards. See Table 4-1 on page 4-2 for a list of Cisco ONS 15454 LTE cards. In CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the card view Provisioning tab.

For detailed information about specific pointer justification count PM parameters, locate the card name in the following sections and review the appropriate definition.

4.4 Performance Monitoring Parameter Definitions

Table 4-2 gives definitions for each type of performance monitoring parameter found in this chapter.

Table 4-2 Performance Monitoring Parameters

Parameter	Definition
AISS-P	AIS Seconds Path (AISS-P) is a count of one-second intervals containing one or more alarm indication signal (AIS) defects.
BES	Block Error Seconds
BBE-PM	Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the optical transport network (OTN) path during the PM time interval.
BBE-SM	Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the OTN section during the PM time interval.
BBER-PM	Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the background block errors ratio recorded in the OTN path during the PM time interval.
BBER-SM	Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the OTN path during the PM time interval.
BIEC	Bit Errors Corrected (BIEC) indicated the number of bit errors corrected in the DWDM trunk line during the PM time interval.
CSS	Controlled Slip Seconds (CSS) indicates the count of the seconds when at least one or more controlled slips have occurred.
CSS-P	Controlled Slip Seconds Path (CSS-P) indicates the count of the seconds when at least one or more controlled slips have occurred.
CVCP-P	Code Violation CP-Bit Path (CVCP-P) is a count of CP-bit parity errors occurring in the accumulation period.
CVCP-PFE	Code Violation CP-Bit Path (CVCP-PFE) is a parameter that is counted when the three far-end block error (FEBE) bits in an M-frame are not all collectively set to 1.
CGV	Code Group Violations (CGV) is a count of received code groups that do not contain a start or end delimiter.
CV-L	Line Code Violation (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
CV-PFE	Far-End STS Path Coding Violations (CV-PFE) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-PFE second register.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
CVP-P	Code Violation Path (CVP-P) is a code violation parameter for M23 applications. CVP-P is a count of P-bit parity errors occurring in the accumulation period.
CV-S	Section Coding Violation (CV-S) is a count of bit interleaved parity (BIP) errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
CV-V	Code Violation VT Layer (CV-V) is a count of the BIP errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe, with each error incrementing the current CV-V second register.
DCG	Date Code Groups (DCG) is a count of received data code groups that do not contain ordered sets.
ESA-P	Count of 1-second intervals with exactly one CRC-6 error and no AIS or severely errored frame (SEF) defects.
ESB-P	Count of 1-second intervals with between 2 and 319 CRC-6 errors and no AIS or SEF.
ESCP-P	Errored Second CP-Bit Path (ESCP-P) is a count of seconds containing one or more CP-bit parity errors, one or more SEF defects, or one or more AIS defects. ESCP-P is defined for the C-bit parity application.
ESCP-PFE	Errored Second CP-bit Path (ESCP-PFE) is a count of one-second intervals containing one or more M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
ES-L	Line Errored Seconds (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (that is, loss of signal) on the line.
ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an ES-P.
ES-PFE	Far-End STS Path Errored Seconds (ES-PFE) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
ES-PM	Path monitoring errored seconds (ES-PM) indicates the errored seconds recorded in the OTN path during the PM time interval.
ESP-P	Errored Second Path (ESP-P) is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
ESR-PM	Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored seconds ratio recorded in the OTN path during the PM time interval.
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored seconds ratio recorded in the OTN section during the PM time interval.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or LOS defect was present.
ES-SM	Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds recorded in the OTN section during the PM time interval.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An AIS-V defect (a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause an ES-V.
FC-L	Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure is declared or when a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.
FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
FC-PFE	Far-End STS Path Failure Counts (FC-PFE) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
FC-PM	Path Monitoring Failure Counts (FC-PM) indicates the failure counts recorded in the OTN path during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) indicates the failure counts recorded in the OTN section during the PM time interval.
IOS	Idle Ordered Sets (IOS) is a count of received packets containing idle ordered sets.
IPC	Number of invalid packets
LBCL-MIN	Laser Bias Current Line—Minimum (LBCL-MIN) is the minimum percentage of laser bias current.
LBCL-AVG	Laser Bias Current Line—Average (LBCL-AVG) is the average percentage of laser bias current.
LBCL-MAX	Laser Bias Current Line—Maximum (LBCL-MAX) is the maximum percentage of laser bias current.
LOFC	Loss of Frame Count
LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
NIOS	Non-Idle Ordered Sets (NIOS) is a count of received packets containing non-idle ordered sets.
NPJC-PDET	Negative Pointer Justification Count, STS Path Detected (NPJC-Pdet-P) is a count of the negative pointer justifications detected on a particular path in an incoming SONET signal.
NPJC-PGEN	Negative Pointer Justification Count, STS Path Generated (NPJC-Pgen-P) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-SEC	
OPR	Optical Power Received (OPR) is the measure of average optical power received as a percentage of the nominal OPT.
OPR-AVG	Average receive optical power (dBm).
OPR-MAX	Maximum receive optical power (dBm).
OPR-MIN	Minimum receive optical power (dBm).
OPT	Optical Power Transmitted (OPT) is the measure of average optical power transmitted as a percentage of the nominal OPT.
OPT-AVG	Average transmit optical power (dBm).
OPT-MAX	Maximum transmit optical power (dBm).
OPT-MIN	Minimum transmit optical power (dBm).
OPWR-AVG	Optical Power—Average (OPWR-AVG) is the measure of average optical power on the unidirectional port.
OPWR-MAX	Optical Power—Maximum (OPWR-MAX) is the measure of maximum value of optical power on the unidirectional port.
OPWR-MIN	Optical Power—Minimum (OPWR-MIN) is the measure of minimum value of optical power on the unidirectional port.
PJC-DIFF	Pointer Justification Count Difference, STS Path (PJCDIFF-P) is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. That is, PJCDiff-P is equal to (PPJC-PGen – NPJC-PGen) – (PPJC-PDet – NPJC-PDet).
PJNEG	Pointer Justification Negative
PJPOS	Pointer Justification Positive
PNPJC-SEC	
PPJC-PDET	Positive Pointer Justification Count, STS Path Detected (PPJC-Pdet-P) is a count of the positive pointer justifications detected on a particular path in an incoming SONET signal.
PPJC-PGEN	Positive Pointer Justification Count, STS Path Generated (PPJC-Pgen-P) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
PPJC-SEC	

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
PSC	In a 1 + 1 protection scheme for a working card, Protection Switching Count (PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.
PSC-R	In a four-fiber BLSR, Protection Switching Count-Ring (PSC-R) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to a working line. A count is only incremented if ring switching is used.
PSC-S	In a four-fiber BLSR, Protection Switching Count-Span (PSC-S) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. A count is only incremented if span switching is used.
PSC-W	For a working line in a two-fiber BLSR, Protection Switching Count-Working (PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line. For a working line in a four-fiber BLSR, PSC-W is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. PSC-W increments on the failed line and PSC-R or PSC-S increments on the active protect line.
PSD	Protection Switching Duration (PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, PSD is a count of the number of seconds that service was carried on the protection line. For the protection line, PSD is a count of the seconds that the line was used to carry service. The PSD PM is only applicable if revertive line-level protection switching is used.
PSD-R	In a four-fiber BLSR, Protection Switching Duration-Ring (PSD-R) is a count of the seconds that the protection line was used to carry service. A count is only incremented if ring switching is used.
PSD-S	In a four-fiber BLSR, Protection Switching Duration-Span (PSD-S) is a count of the seconds that the protection line was used to carry service. A count is only incremented if span switching is used.
SASCP-P	SEF/AIS Seconds CP-Bit Path (SASCP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SAS-P	SEF/AIS Seconds (SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
SASP-P	SEF/AIS Seconds Path (SASP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SESCP-P	Severely Errored Seconds CP-Bit Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
SEFS	Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or loss of frame (LOF) defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect.
SESCP-P	Severely Errored Seconds CP-Bit Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
SESCP-PFE	Severely Errored Second CP-Bit Path (SESCP-PFE) is a count of one-second intervals containing one or more 44 M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
SES-L	Line Severely Errored Seconds (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an SES-P.
SES-PFE	Far-End STS Path Severely Errored Seconds (SES-PFE) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an SES-PFE.
SES-PM	Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely errored seconds recorded in the OTN path during the PM time interval.
SESP-P	Severely Errored Seconds Path (SESP-P) is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely errored seconds recorded in the OTN section during the PM time interval.
SESR-PM	Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the severely errored seconds ratio recorded in the OTN path during the PM time interval.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
SESR-SM	Section Monitoring Severely Errored Seconds Ratio (SESR-SM) indicates the severely errored seconds ratio recorded in the OTN section during the PM time interval.
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause SES-V.
UAS-L	Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.
UASCP-P	Unavailable Seconds CP-Bit Path (UASCP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS-3 path becomes unavailable when ten consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.
UASCP-PFE	Unavailable Second CP-Bit Path (UASCP-PFE) is a count of one-second intervals when the DS-3 path becomes unavailable. A DS-3 path becomes unavailable when ten consecutive far-end CP-bit SESs occur. The ten CP-bit SESs are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds occur with no CP-bit SESs. The ten seconds with no CP-bit SESs are excluded from unavailable time.
UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.
UAS-PFE	Far-End STS Path Unavailable Seconds (UAS-PFE) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-PFEs, and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-PFEs.
UAS-PM	Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval.
UASP-P	Unavailable Seconds Path (UASP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS-3 path becomes unavailable when ten consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.

Table 4-2 Performance Monitoring Parameters (continued)

Parameter	Definition
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval.
UAS-V	Unavailable Seconds VT Layer (UAS-V) is a count of the seconds when the VT path was unavailable. A VT path becomes unavailable when ten consecutive seconds occur that qualify as SES-Vs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Vs.
UNC-WORDS	The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.
VPC	Number of valid packets

4.5 DS-1 Facility Data Link Performance Monitoring

Facility Data Link (FDL) performance monitoring enables an ONS 15454 DS1N-14 card to calculate and report DS-1 error rate performance measured at both the near-end and far-end of the FDL. The far-end information is reported as received on the FDL in a performance report message (PRM) from an intelligent channel service unit (CSU).

To monitor DS-1 FDL PM values, the DS-1 must be set to use Extended Superframe (ESF) format and the FDL must be connected to an intelligent CSU. For procedures on provisioning ESF on the DS1N-14 card, refer to the *Cisco ONS 15454 Procedure Guide*.

The monitored DS-1 FDL PM parameters are CV-PFE, ES-PFE, ESA-PFE, ESB-PFE, SES-PFE, SEFS-PFE, CSS-PFE, UAS-PFE, FC-PFE, and ES-LFE. For detailed information about specific DS-1 FDL PM parameters, locate the DS1N-14 card name in the following sections and review the appropriate definition.

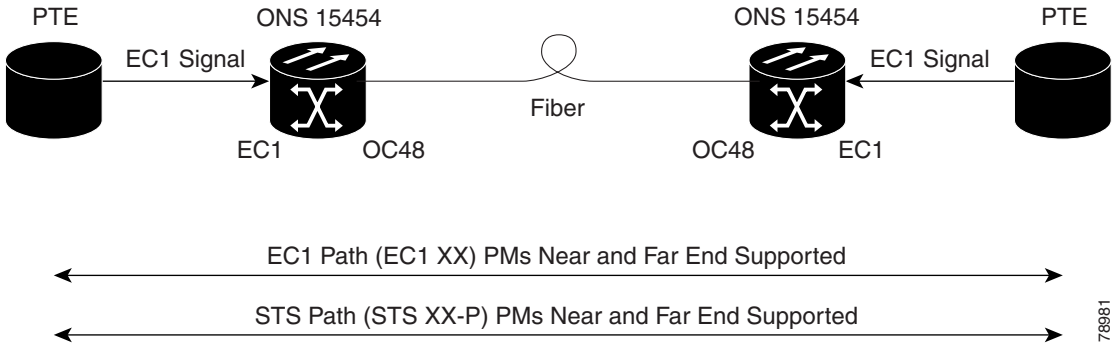
4.6 Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the EC1-12, DS1-14, DS1N-14, DS3-12, DS3-12E, DS3N-12, DS3N-12E, DS3XM-6, DS3XM-12, and DS3/EC1-48 cards.

4.6.1 EC1-12 Card Performance Monitoring Parameters

Figure 4-1 shows signal types that support near-end and far-end PMs. Figure 4-2 shows where overhead bytes detected on the application specific integrated circuits (ASICs) produce performance monitoring parameters for the EC1-12 card.

Figure 4-1 Monitored Signal Types for the EC1-12 Card



Note The XX in Figure 4-1 represents all PMs listed in Table 4-3 with the given prefix and/or suffix.

Figure 4-2 PM Read Points on the EC1-12 Card

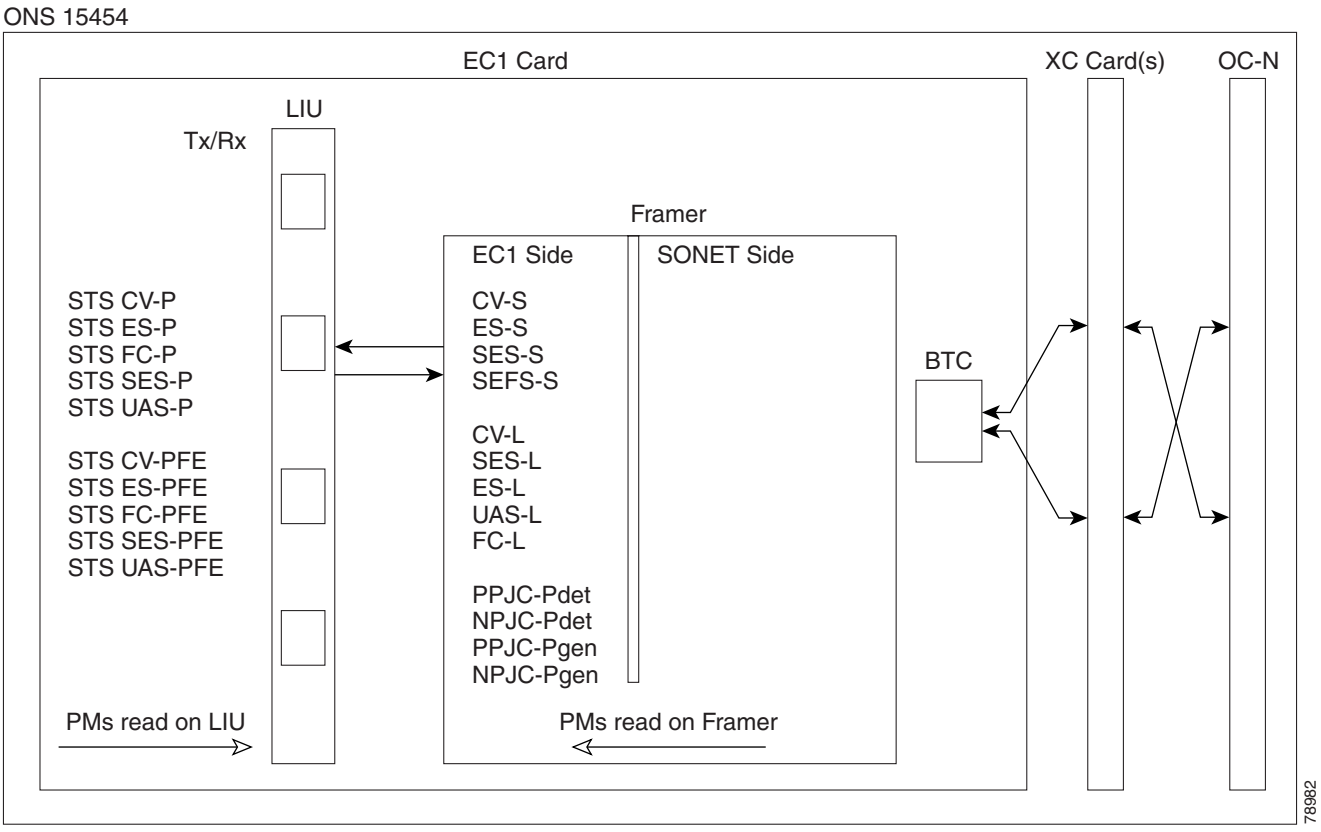


Table 4-3 lists the PM parameters for the EC1-12 cards.

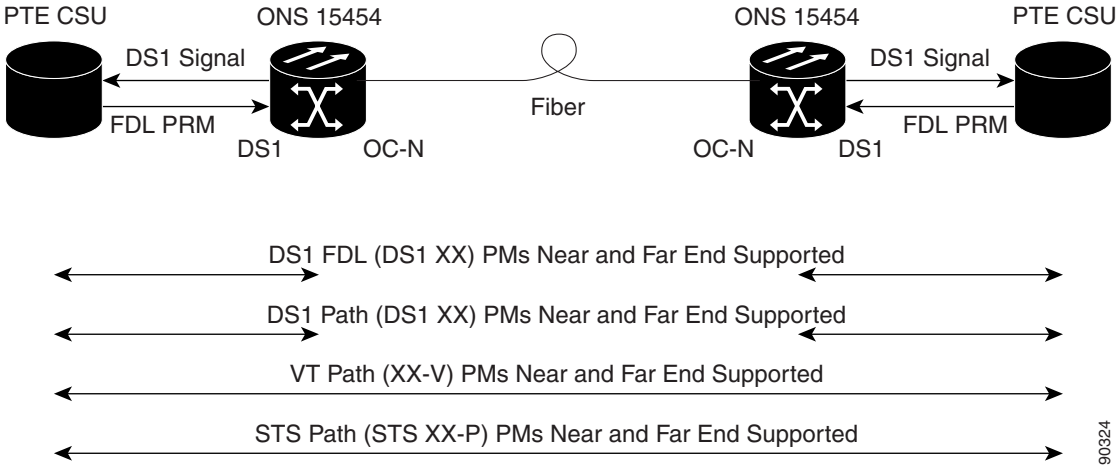
Table 4-3 EC1 Card PMs

Section (NE)	Line (NE)	STS Path (NE)	Line (FE)	STS Path (FE)
CV-S ES-S SES-S SEFS-	CV-L ES-L SES-L UAS-L FC-L	CV-P ES-P SES-P UAS-P FC-P PPJC-PDET NPJC-PDET PPJC-PGEN NPJC-PGEN PNPJC-SEC NPJC-SEC PJC-DIFF	CV-LFE ES-LFE SES-LFE UAS-LFE FC-LFE	CV-PFE ES-PFE SES-PFE UAS-PFE FC-PFE

4.6.2 DS1-14 and DS1N-14 Card Performance Monitoring Parameters

Figure 4-3 shows the signal types that support near-end and far-end PMs.

Figure 4-3 Monitored Signal Types for the DS1-14 and DS1N-14 Cards



Note The XX in Figure 4-3 represents all PMs listed in Table 4-4 with the given prefix and/or suffix.

Figure 4-4 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS1-14 and DS1N-14 cards.

Figure 4-4 PM Read Points on the DS1-14 and DS1N-14 Cards

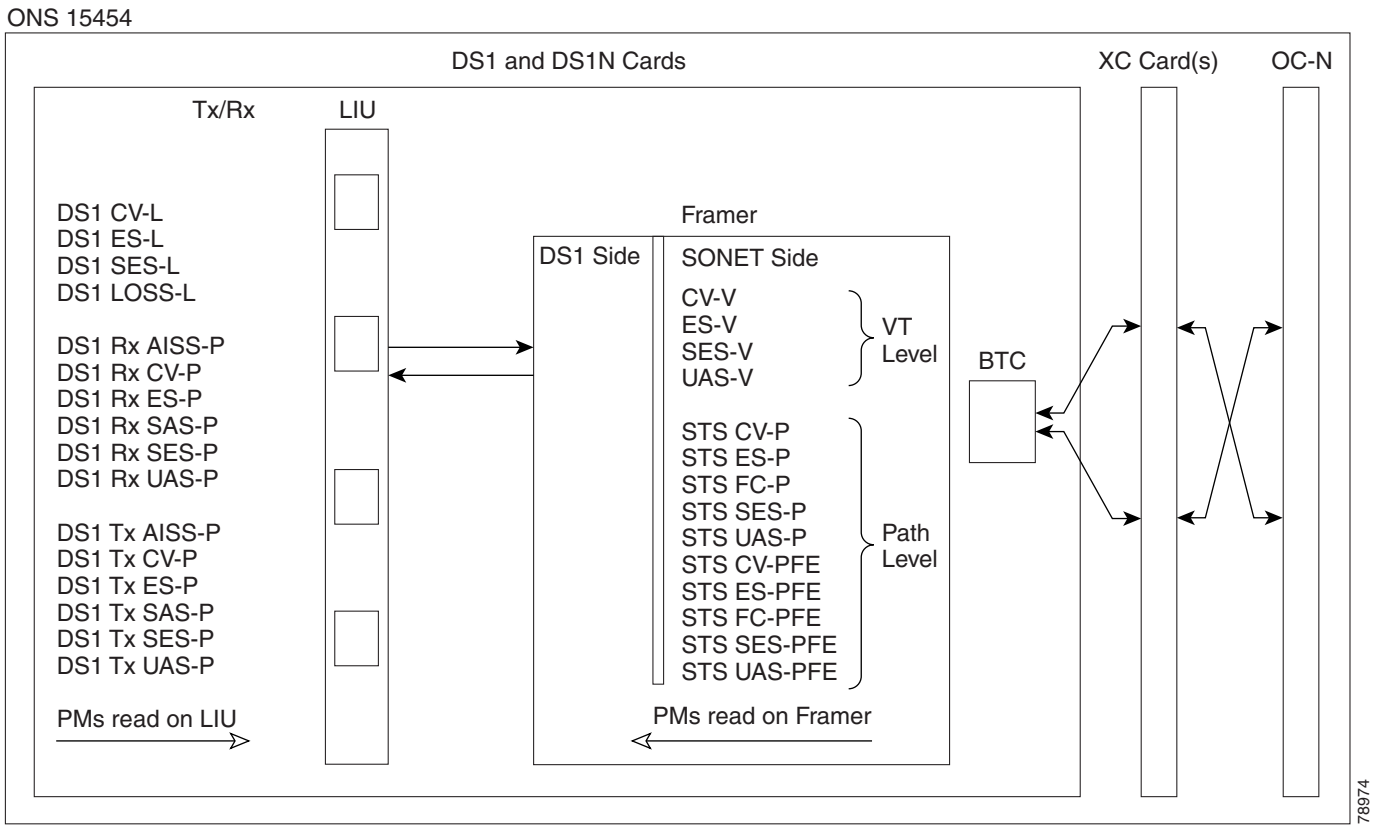


Table 4-4 describes the PM parameters for the DS1-14 and DS1N-14 cards.

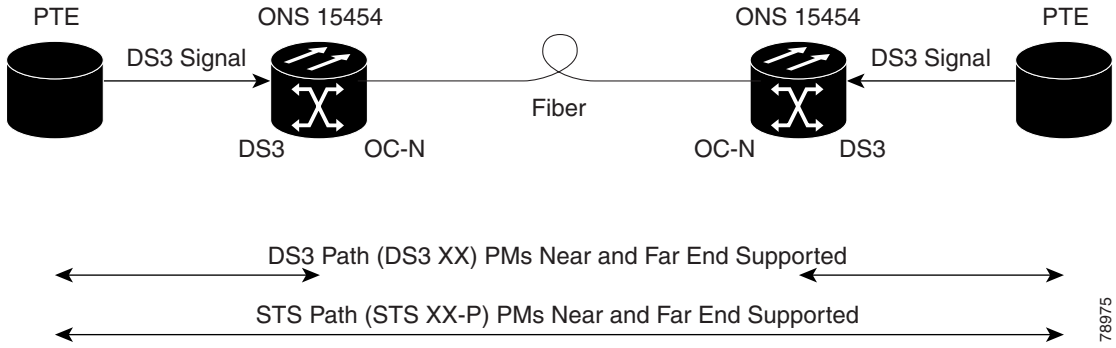
Table 4-4 DS1-14 and DS1N-14 Card PMs

Line (NE)	Line (FE)	Rx Path (NE)	Tx Path (NE)	VT Path (NE)	STS Path (NE)	Rx Path (FE)	V (FE)	STS Path (FE)
CV-L	CV-LFE	AISS-P	AISS-P	CV-V	CV-P	ES-PFE	CV-VFE	CV-P
ES-L	ES-LFE	CV-P	CV-P	ES-V	ES-P	ESA-PFE	ES-VFE	ES-P
SES-L		ES-P	ES-P	SES-V	SES-P	ESB-PFE	SES-VFE	SES-P
LOSS-L		SAS-P	SAS-P	UAS-V	UAS-P	CV-PFE	UAS-VFE	UAS-P
		SES-P	SES-P		FC-P	CSS-PFE		FC-P
		UAS-P	UAS-P			SEFS-PFE		
						SES-PFE		
						UAS-PFE		

4.6.3 DS3-12 and DS3N-12 Card Performance Monitoring Parameters

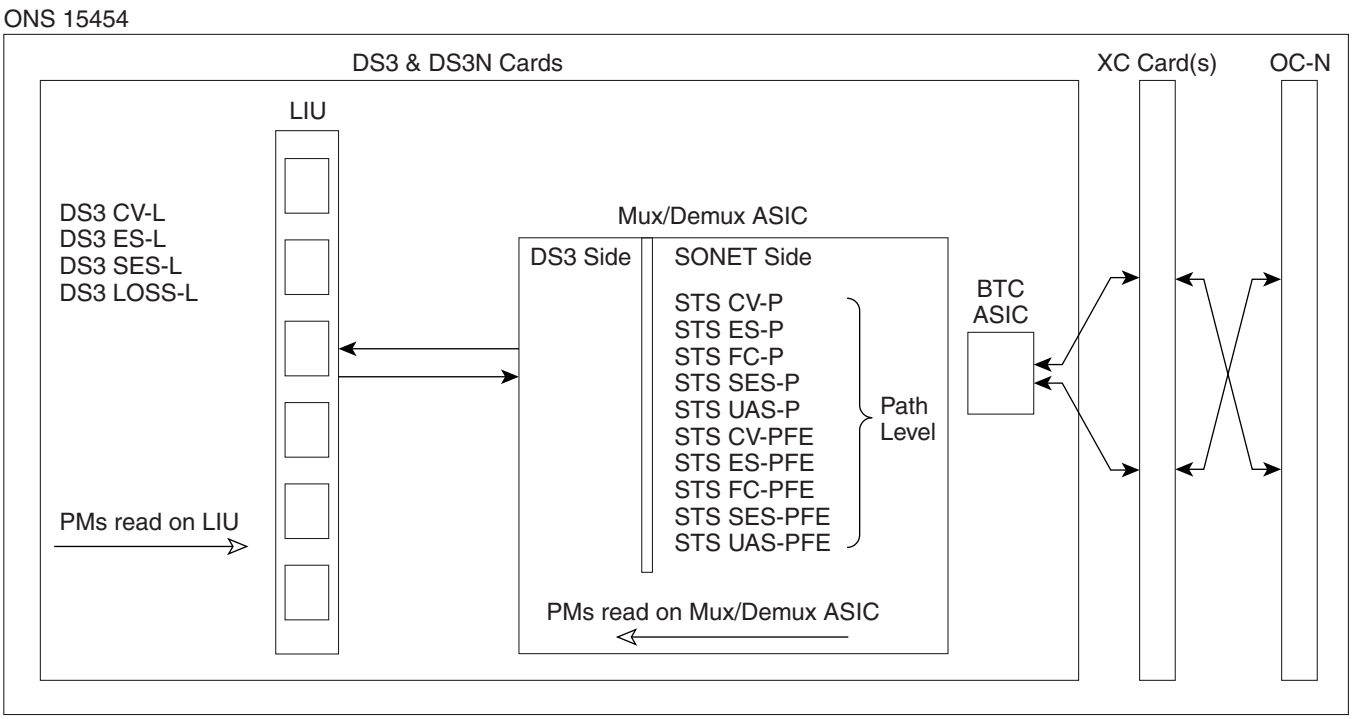
Figure 4-5 shows the signal types that support near-end and far-end PMs. Figure 4-6 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3-12 and DS3N-12 cards.

Figure 4-5 Monitored Signal Types for the DS3-12 and DS3N-12 Cards



Note The XX in Figure 4-5 represents all PMs listed in Table 4-5 with the given prefix and/or suffix.

Figure 4-6 PM Read Points on the DS3-12 and DS3N-12 Cards



The PM parameters for the DS3-12 and DS3N-12 cards are described in Table 4-5.

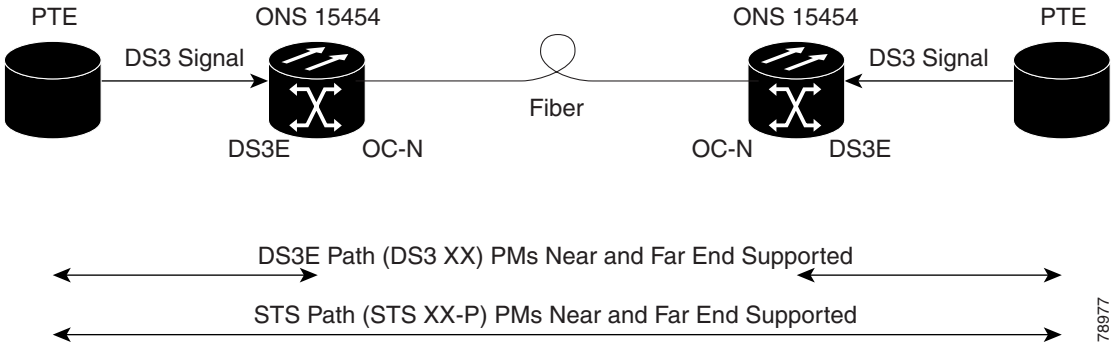
Table 4-5 DS3-12 and DS3N-12 Card PMs

Line (NE)	STS Path (NE)	STS Path (FE)
CV-L	CV-P	CV-PFE
ES-0L	ES-P	ES-PFE
SES-L	SES-P	SES-PFE
LOSS-L	UAS-P	UAS-PFE
	FC-P	FC-PFE

4.6.4 DS3-12E and DS3N-12E Card Performance Monitoring Parameters

Figure 4-7 shows the signal types that support near-end and far-end PMs.

Figure 4-7 Monitored Signal Types for the DS3-12E and DS3N-12E Cards



Note The XX in Figure 4-7 represents all PMs listed in Table 4-6 with the given prefix and/or suffix.

Figure 4-8 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3-12E and DS3N-12E cards.

Figure 4-8 PM Read Points on the DS3-12E and DS3N-12E Cards

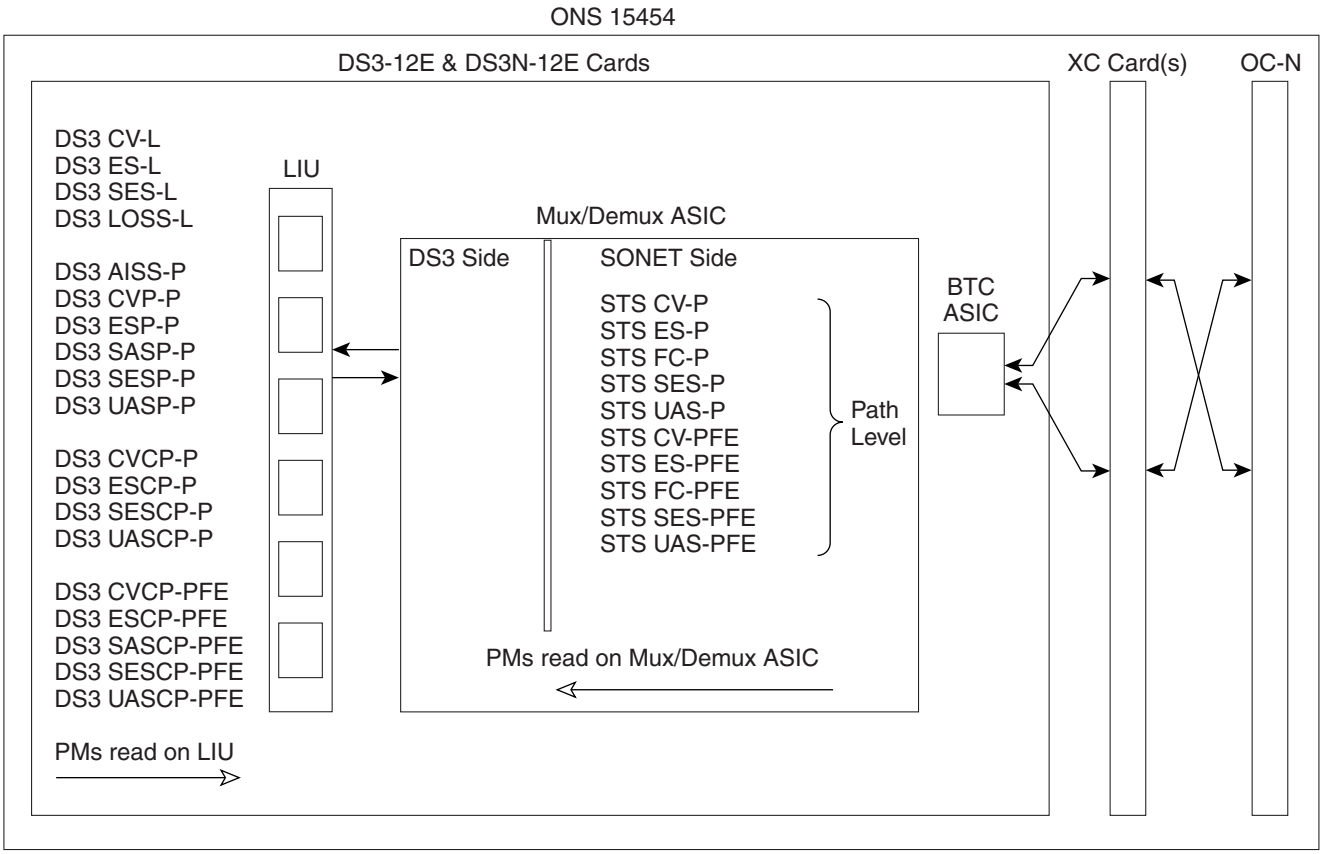


Table 4-6 describes the PM parameters for the DS3-12E and DS3N-12E cards.

Table 4-6 DS3-12E and DS3N-12E Card PMs

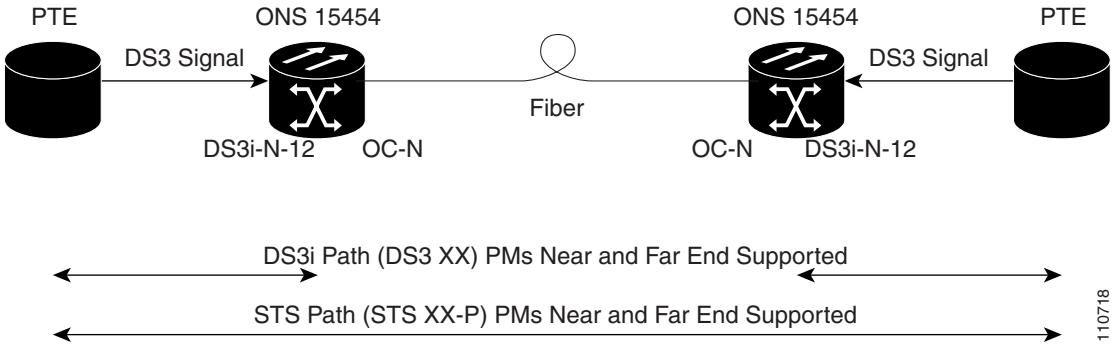
Line (NE)	Path (NE)	STS Path (NE)	Path (FE)[1]	STS Path (FE)
CV-L	AISS-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CV-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ES-P	SES-P	SASCP-PFE	SES-PFE
LOSS-L	SAS-P[2]	UAS-P	SESCP-PFE	UAS-PFE
	SES-P	FC-P	UASCP-PFE	FC-PFE
	UAS-P			
	CVCP-P			
	ESCP-P			
	SESCP-P			
	UASCP-P			

1. The C-bit PMs (PMs that end in "CPP") are applicable only if the line format is C-bit.
2. DS3(N)-3E cards support SAS-P only on the receive (Rx) path.

4.6.5 DS3i-N-12 Card Performance Monitoring Parameters

Figure 4-9 shows the signal types that support near-end and far-end PMs.

Figure 4-9 Monitored Signal Types for the DS3i-N-12 Cards



Note The XX in Figure 4-9 represents all PMs listed in Table 4-7 with the given prefix and/or suffix.

Figure 4-10 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3i-N-12 cards.

Figure 4-10 PM Read Points on the DS3i-N-12 Cards

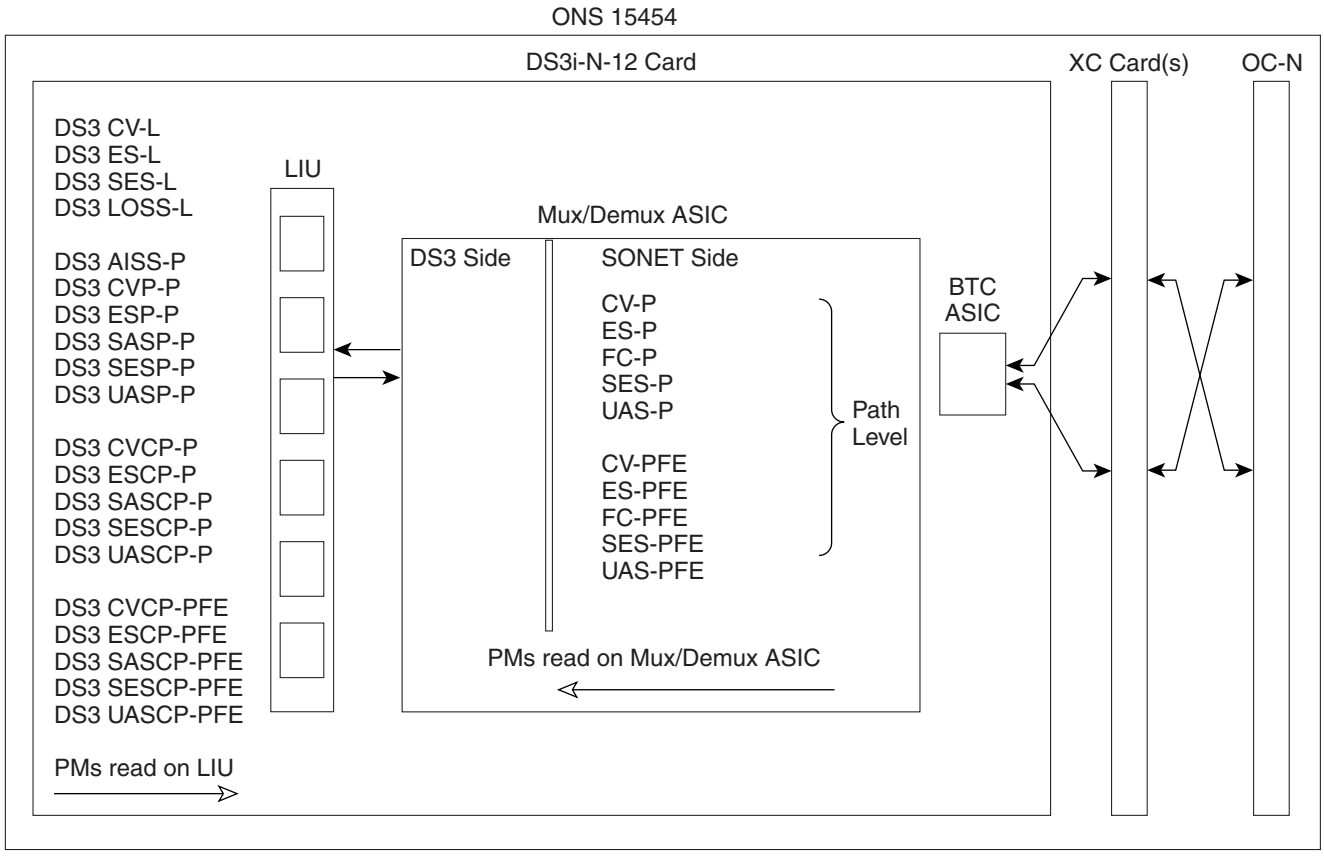


Table 4-7 describes the PM parameters for the DS3-12E and DS3N-12E cards.

Table 4-7 DS3i-N-12 Card PMs

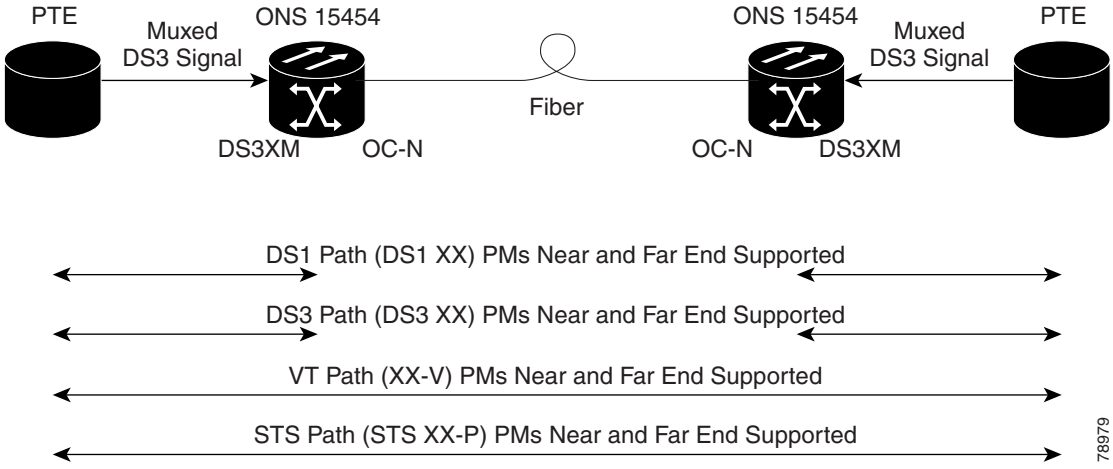
Line (NE)	Path (NE)	STS Path (NE)	Path (FE)[1]	STS Path (FE)
CV-L	AISS-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CVP-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ESP-P	SES-P	SASCP-PFE	SES-PFE
LOSS-L	SASP-P[2]	UAS-P	SESCP-PFE	UAS-PFE
	SESP-P	FC-P	UASCP-PFE	FC-PFE
	UASP-P			
	CVCP-P			
	ESCP-P			
	SASP-P			
	SESCP-P			
	UASCP-P			

1. The C-bit PMs (PMs that end in "CPP") are applicable only if line format is C-bit.
2. DS3i-N-12 cards support SAS-P only on the Rx path.

4.6.6 DS3XM-6 Card Performance Monitoring Parameters

Figure 4-11 shows the signal types that support near-end and far-end PMs.

Figure 4-11 Monitored Signal Types for the DS3XM-6 Card



Note The XX in Figure 4-11 represents all PMs listed in Table 4-8 with the given prefix and/or suffix.

Figure 4-12 shows where the overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3XM-6 card.

Figure 4-12 PM Read Points on the DS3XM-6 Card

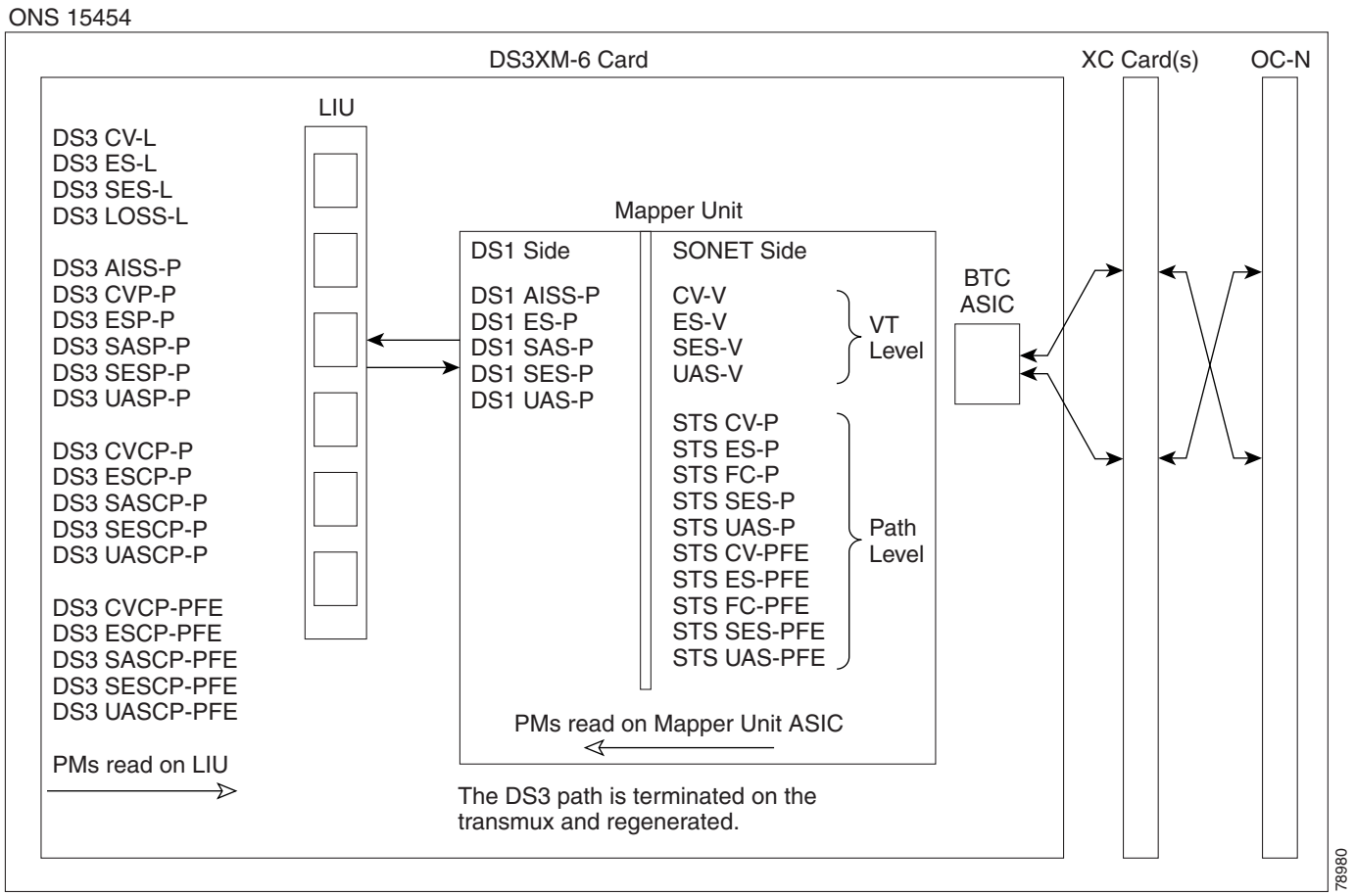


Table 4-8 lists the PM parameters for the DS3XM-6 cards.

Table 4-8 DS3XM-6 Card PMs

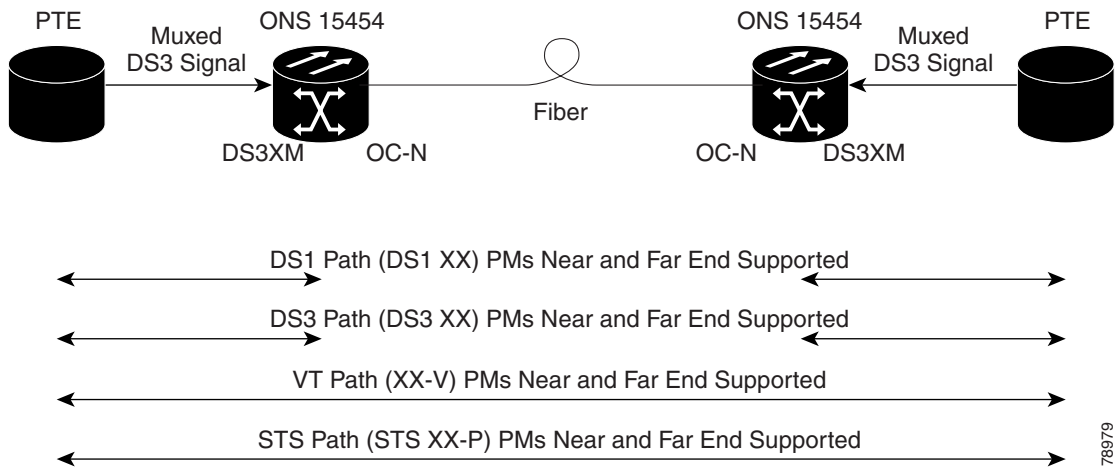
DS3 Line (NE)	DS3 Path (NE)[1]	DS1 Path (NE)	VT Path (NE)	STS Path (NE)	DS3 Path (FE)[1]	VT Path (FE)	STS Path (FE)
CV-L	AISS-P	AISS-P	CV-V	CV-P	CVCP-PFE	CV-VFE	CV-PFE
ES-L	CV-P	ES-P	ES-V	ES-P	ESCP-PFE	ES-VFE	ES-PFE
SES-L	ES-P	SAS-P[2]	SES-V	SES-P	SASCP-PFE	SES-VFE	SES-PFE
LOSS-L	SAS-P[2]	SES-P	UAS-V	UAS-P	SESCP-PFE	UAS-VFE	UAS-PFE
	SES-P	UAS-P		FC-P	UASCP-PFE		FC-PFE
	UAS-P						
	ESCP-P						
	SESCP-P						
	UASCP-P						
	CVCP-P						

1. The C-bit PMs (PMs that end in “CPP”) are applicable only if line format is C-bit.
2. DS3XM-6 cards support SAS-P only on the Rx path.

4.6.7 DS3XM-12 Card Performance Monitoring Parameters

Figure 4-13 shows the signal types that support near-end and far-end PMs.

Figure 4-13 Monitored Signal Types for the DS3XM-12 Card



Note The XX in Figure 4-13 represents all PMs listed in Table 4-9 with the given prefix and/or suffix.

Figure 4-12 shows where the overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3XM-12 card.

Figure 4-14 PM Read Points on the DS3XM-12 Card

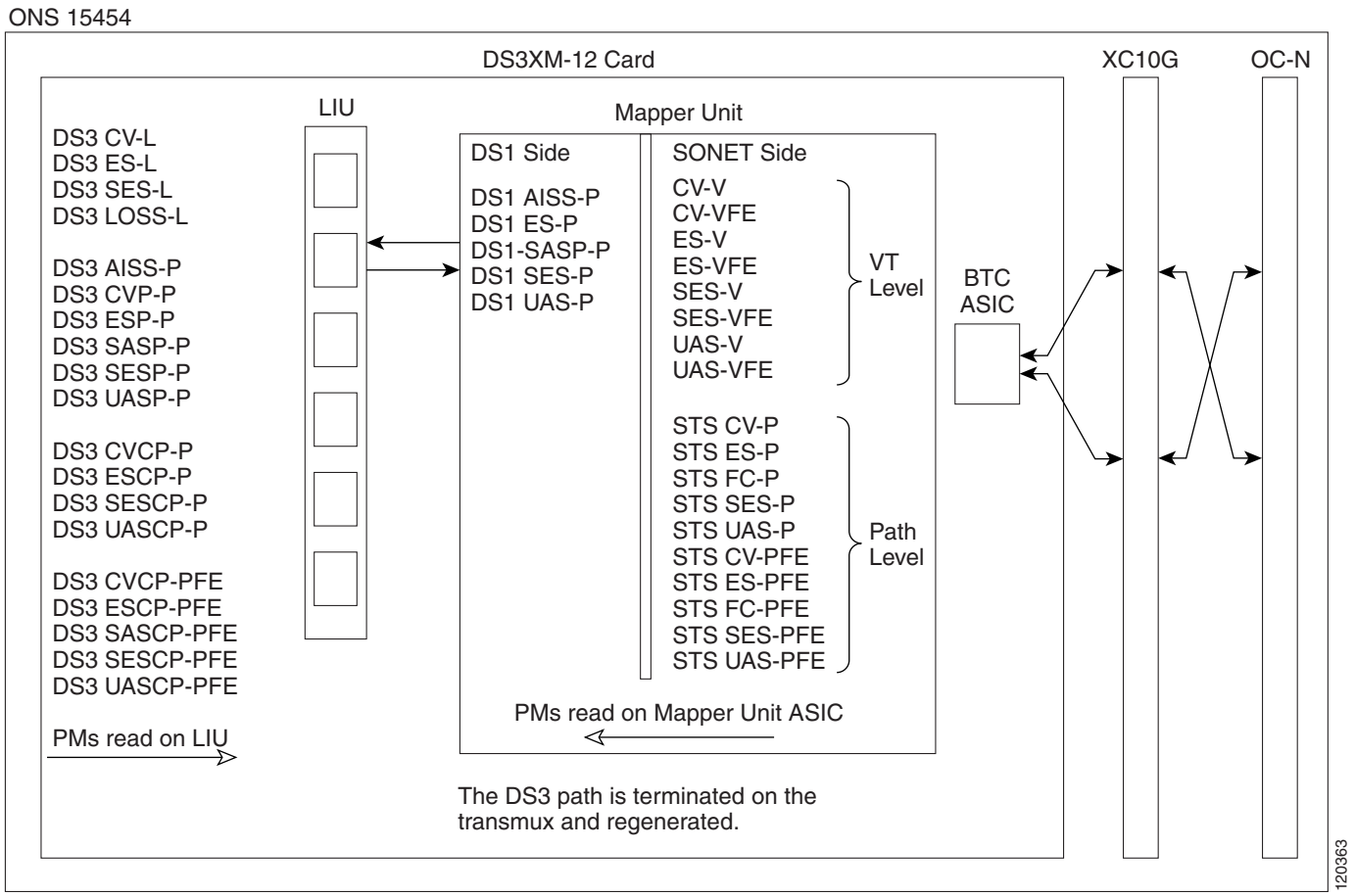


Table 4-9 lists the PM parameters for the DS3XM-12 cards.

Table 4-9 DS3XM-12 Card PMs

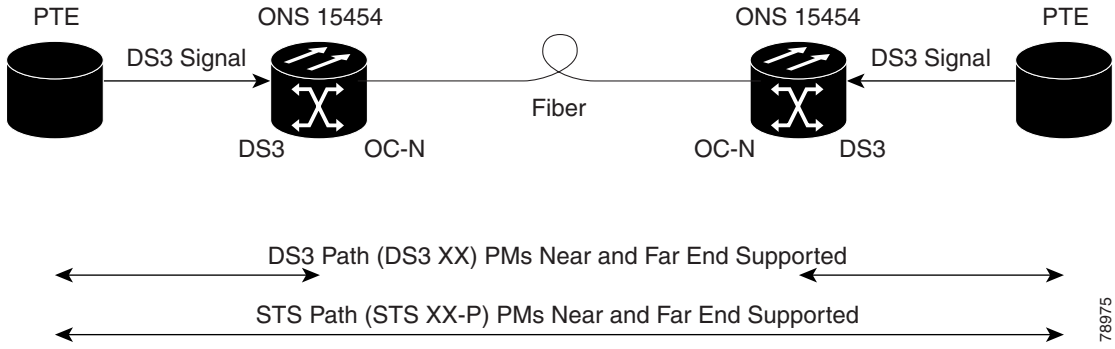
DS3 Line (NE)	DS3 Path (NE)[1]	DS1 Path (NE)	VT Path (NE)	STS Path (NE)	DS3 Path (FE)[1]	VT Path (FE)	STS Path (FE)	BFDL (FE)
CV-L	AISS-P	AISS-P	CV-V	CV-P	CVCP-PFE	CV-VFE	CV-PFE	CSS
ES-L	CV-P	ES-P	ES-V	ES-P	ESCP-PFE	ES-VFE	ES-PFE	ES
SES-L	ES-P	SAS-P[2]	SES-V	SES-P	SASCP-PFE	SES-VFE	SES-PFE	SES
LOSS-L	SAS-P[2]	SES-P	UAS-V	UAS-P	SESCP-PFE	UAS-VFE	UAS-PFE	BAS
	SES-P	UAS-P		FC-P	UASCP-PFE		FC-PFE	UAS
	UAS-P							LOFC
	ESCP-P							
	SESCP-P							
	UASCP-P							
	CVCP-P							

1. The C-bit PMs (PMs that end in “CPP”) are applicable only if line format is C-bit.
2. DS3XM-12 cards support SAS-P only on the Rx path.

4.6.8 DS3/EC1-48 Card Performance Monitoring Parameters

Figure 4-15 shows the signal types that support near-end and far-end PMs.

Figure 4-15 Monitored Signal Types for the DS3/EC1-48 Card



Note The XX in Figure 4-15 represents all PMs listed in Table 4-10 with the given prefix and/or suffix.

Figure 4-16 shows where the overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3/EC1-48 card.

Figure 4-16 PM Read Points on the DS3/EC1-48 Card

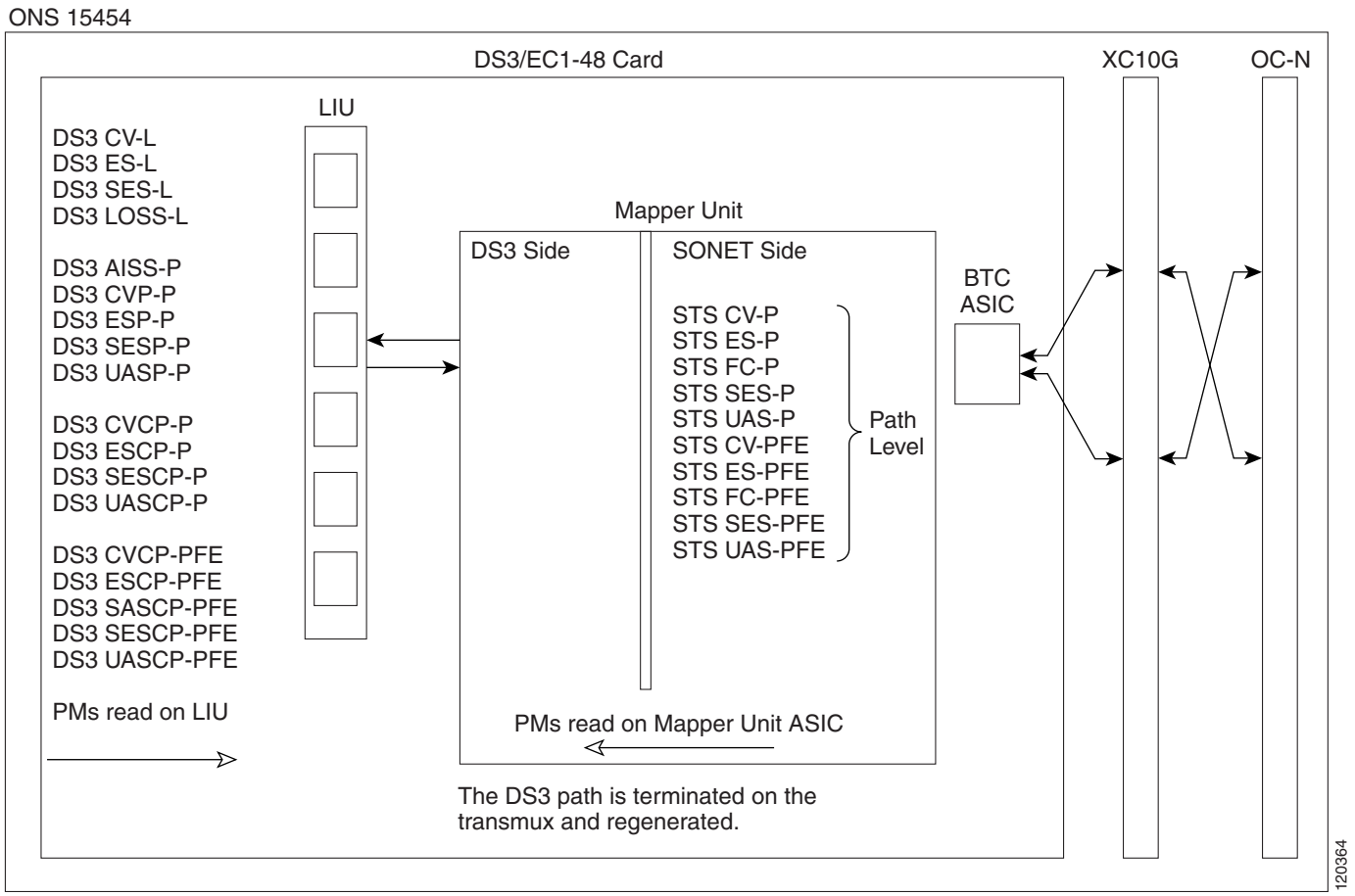


Table 4-10 lists the PM parameters for the DS3/EC1-48 cards.

Table 4-10 DS3/EC1-48 Card PMs

DS3 Line (NE)	DS3 Path (NE)[1]	STS Path (NE)	DS3 Path (FE)[1]	STS Path (FE)
CV-L	AISS-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CV-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ES-P	SES-P	SESCP-PFE	SES-PFE
LOSS-L	SAS-P[2]	UAS-P	UASCP-PFE	UAS-PFE
	SES-P	FC-P		FC-PFE
	UAS-P			
	ESCP-P			
	SESCP-P			
	UASCP-P			
	CVCP-P			

1. The C-bit PMs (PMs that end in “CPP”) are applicable only if line format is C-bit.
2. DS3/EC1-48 cards support SAS-P only on the Rx path.

4.7 Performance Monitoring for Ethernet Cards

The following sections define performance monitoring parameters and definitions for the ONS 15454 E-Series, G-Series, and ML-Series Ethernet cards.

4.7.1 E-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The E-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

4.7.2 E-Series Ethernet Statistics Window

The Ethernet statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs.

Table 4-11 defines the E-Series Ethernet card Statistics parameters.

Table 4-11 E-Series Ethernet Statistics Parameters

Parameter	Definition
Link Status	Indicates whether link integrity is present; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets received with a Frame Check Sequence (FCS) error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with alignment errors. Alignment errors are received incomplete frames.
Rx Runts	Number of undersized packets received with bad cyclic redundancy check (CRC) errors.
Rx Shorts	Number of undersized received packets with good CRC errors.
Rx Oversized + Jabbers	Measures oversized packets and jabbers. Size is greater than 1522 errors regardless of CRC errors.
Tx Collisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
Tx Late Collisions	Number of frames that were not transmitted since they encountered a collision outside of the normal collision window (late collision events should occur only rarely).

Table 4-11 E-Series Ethernet Statistics Parameters (continued)

Parameter	Definition
Tx Excessive Collisions	Number of consecutive collisions.
Tx Deferred	Number of packets deferred.

4.7.3 E-Series Ethernet Utilization Window

The Utilization window shows the percentage of transmit (Tx) and receive (Rx) line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the E-Series port. However, if the E-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the E-Series and the peer Ethernet device attached directly to the E-Series port.

The **Utilization** window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for E-Series Ethernet cards is shown in Table 4-12.

Table 4-12 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note The E-Series Ethernet card is a Layer 2 device or switch and supports Trunk Utilization statistics. The Trunk Utilization statistics are similar to the Line Utilization statistics, but shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. The Trunk Utilization statistics are accessed via the card view Maintenance tab.

4.7.4 E-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-13. The listed parameters are defined in Table 4-11 on page 4-25.

Table 4-13 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

4.7.5 G-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The G-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

4.7.6 G-Series Ethernet Statistics Window

The Ethernet statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The G-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the G-Series card.

Table 4-14 defines the G-Series Ethernet card Statistics parameters.

Table 4-14 G-Series Ethernet Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a FCS error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with received incomplete frames.
Rx Runts	Number of undersized packets received with bad CRC errors.
Rx Shorts	Measures undersized packets received with good CRC errors.
Rx Jabbers	The total number of frames received that exceed the 1548-byte maximum and contain CRC errors.

Table 4-14 G-Series Ethernet Statistics Parameters (continued)

Parameter	Definition
Rx Giants	Number of packets received that are greater than 1530 bytes in length.
Rx Pause Frames	Number of received Ethernet IEEE 802.3z pause frames.
Tx Pause Frames	Number of transmitted IEEE 802.3z pause frames.
Rx Pkts Dropped Internal Congestion	Number of received packets dropped due to overflow in G-Series frame buffer.
Tx Pkts Dropped Internal Congestion	Number of transmit queue drops due to drops in the G-Series frame buffer.
HDLC Errors	High-level data link control (HDLC) errors received from SONET/SDH (see Note).
Rx Unicast Packets	Number of unicast packets received since the last counter reset.
Tx Unicast Packets	Number of unicast packets transmitted.
Rx Multicast Packets	Number of multicast packets received since the last counter reset.
Tx Multicast Packets	Number of multicast packets transmitted.
Rx Broadcast Packets	Number of broadcast packets received since the last counter reset.
Tx Broadcast Packets	Number or broadcast packets transmitted.

Note Do not use the high level data link control (HDLC) errors counter to count the number of frames dropped because of HDLC errors, because each frame can fragment into several smaller frames during HDLC error conditions and spurious HDLC frames can be generated. If HDLC error counters are incrementing when no SONET path problems should be present, it might indicate a problem with the quality of the SONET path. For example, a SONET protection switch generates a set of HDLC errors. However, the actual values of these counters are less significant than the fact that they are changing.

4.7.7 G-Series Ethernet Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the G-Series port. However, if the G-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the G-Series and the peer Ethernet device attached directly to the G-Series port.

The **Utilization** window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for G-Series Ethernet cards is shown in Table 4-15.

Table 4-15 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note Unlike the E-Series cards, the G-Series cards do not have a display of Trunk Utilization statistics because the G-Series card is not a Layer 2 device or switch.

4.7.8 G-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-16. The listed parameters are defined in Table 4-14 on page 4-27.

Table 4-16 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

4.7.9 ML-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information for line-level parameters and historical Ethernet statistics. The ML-Series Ethernet performance information is divided into the Ether Ports and POS (Packet over SONET/SDH) Ports tabbed windows within the card view Performance tab window.

Table 4-17 defines the ML-Series Ethernet card Ether Ports PM parameters.

Table 4-17 ML-Series Ether Ports PM Parameters

Parameter	Definition
Rx Bytes	Number of bytes received since the last counter reset.
Rx Packets	Number of packets received since the last counter reset.
Rx Unicast Packets	Number of unicast packets received since the last counter reset.
Rx Multicast Packets	Number of multicast packets received since the last counter reset.
Rx Broadcast Packets	Number of broadcast packets received since the last counter reset.
Rx Giants	Number of packets received that are greater than 1530 bytes in length.
Rx Total Errors	Total number of receive errors.
Rx FCS Errors	Number of packets received with an FCS error.
Rx Runts	Total number of frames received that are less than 64 bytes in length and have a CRC error.
Rx Jabbers	Total number of frames received that exceed the maximum 1548 bytes and contain CRC errors.
Rx Align Errors	Number of received packets with alignment errors.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Unicast Packets	Number of unicast packets transmitted.
Tx Multicast Packets	Number of multicast packets transmitted.
Tx Broadcast Packets	Number or broadcast packets transmitted.
Tx Giants	Number of packets transmitted that are greater than 1548 bytes in length.
Tx Collisions	Number of transmitted packets that collided.
Port Drop Counts	Number of received frames dropped at the port level.
Rx Pause Frames	Number of received pause frames.
Rx Threshold Oversizes	Number of received packets larger than the ML-Series RMON threshold.
Rx GMAC Drop Counts	Number of received frames dropped by MAC module.
Tx Pause Frames	Number of transmitted pause frames.

Table 4-18 defines the ML-Series Ethernet card POS Ports parameters.

Table 4-18 ML-Series POS Ports Parameters

Parameter	Definition
Rx Pre Hdlc Bytes	Number of bytes received prior to the bytes HLDC encapsulation by the policy engine.
Rx Post Hdlc Bytes	Number of bytes received after the bytes HLDC encapsulation by the policy engine.
Rx Packets	Number of packets received since the last counter reset.
Rx Normal Packets	Number of packets between the minimum and maximum packet size received.

Table 4-18 ML-Series POS Ports Parameters (continued)

Parameter	Definition
Rx Shorts	Number of packets below the minimum packet size received.
Rx Runts	Total number of frames received that are less than 64 bytes in length and have a CRC error.
Rx Longs	Counter for the number of received frames that exceed the maximum valid packet length of 1518 bytes.
Rx Total Errors	Total number of receive errors.
Rx CRC Errors	Number of packets received with a CRC error.
Rx Input Drop Packets	Number of received packets dropped before input.
Rx Input Abort Packets	Number of received packets aborted before input.
Tx Pre Hdlc Bytes	Number of bytes transmitted prior to the bytes HLDC encapsulation by the policy engine.
Tx Post Hdlc Bytes	Number of bytes transmitted after the bytes HLDC encapsulation by the policy engine.
Tx Packets	Number of packets transmitted since the last counter reset.
Port Drop Counts	Number of received frames dropped at the port level.

4.7.10 CE-100T-8 Card Ethernet Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The CE-100T-8 card Ethernet performance information is divided into Ether Ports and POS Ports tabbed windows within the card view Performance tab window.

4.7.10.1 CE-100T-8 Card Ether Port Statistics Window

The Ether Ports statistics window lists Ethernet parameters at the line level. The Ether Ports Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the CE-100T-8 card.

During each automatic cycle, whether auto-refreshed or manually refreshed (using the Refresh button), statistics are added cumulatively and are not immediately adjusted to equal total received packets until testing ends. To see the final PM count totals, allow a few moments for the PM window statistics to finish testing and update fully. PM counts are also listed in the CE-100T-8 card Performance > History window.

Table 4-19 defines the CE-100T-8 card Statistics parameters.

Table 4-19 CE-100T-8 Ethernet Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.

Table 4-19 CE-100T-8 Ethernet Statistics Parameters (continued)

Parameter	Definition
Rx Unicast Packets	Number of unicast packets received since the last counter reset.
Tx Unicast Packets	Number of unicast packets transmitted since the last counter reset.
Rx Multicast Packets	Number of multicast packets received since the last counter reset.
Tx Multicast Packets	Number of multicast packets transmitted since the last counter reset.
Rx Broadcast Packets	Number of broadcast packets received since the last counter reset.
Tx Broadcast Packets	Number of broadcast packets transmitted since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Packets	Number of packets received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Rx Errors	The number of inbound packets (or transmission units) that contained errors, preventing them from being delivered to a higher-layer protocol.
Rx Runts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Rx Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
Rx Giants	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Tx Utilization	Same as Rx Utilization, except calculated over the Tx line bandwidth.
Rx Alignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
Rx FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.

4.7.10.2 CE-100T-8 Card Ether Ports Utilization Window

The Ether Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Ether Ports Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate.

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate.

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for CE-100T-8 Ethernet cards is shown in Table 4-20.

Table 4-20 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

4.7.10.3 CE-100T-8 Card Ether Ports History Window

The Ether Ports History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the Ether Ports History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-21. The listed parameters are defined in Table 4-14 on page 4-27.

Table 4-21 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

4.7.10.4 CE-100T-8 Card POS Ports Statistics Parameters

The POS Ports statistics window lists POS parameters at the line level.

Table 4-22 defines the CE-100T-8 card POS Ports parameters.

Table 4-22 CE-100T-8 Card POS Ports Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Rx Octets	Number of bytes received (from the SONET/SDH path) prior to the bytes undergoing HLDC decapsulation by the policy engine.
Tx Octets	Number of bytes transmitted (to the SONET/SDH path) after the bytes undergoing HLDC encapsulation by the policy engine.

Table 4-22 CE-100T-8 Card POS Ports Parameters (continued)

Parameter	Definition
Rx Frames / Packets	Receive data frames.
Tx Frames / Packets	Transmit data frames.
Rx Octets	Received data octets.
Tx Octets	Transmit data octets.
Rx CRC Errors	Receive data frames with payload CRC errors.
Rx MBit Errors	Receive frames with multi bit errors (cHEC, tHEC, eHEC).
Rx SBit Errors	Receive frames with single bit errors (cHEC, tHEC, eHEC).
Rx Type Invalid	Receive frames with invalid type (PTI, EXI, UPI).
Rx CID Invalid	Receive frames with invalid CID.

4.7.10.5 CE-100T-8 Card POS Ports Utilization Window

The POS Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the POS ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate.

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate.

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps).

Refer to Table 4-20 for maxBaseRate values for STS Circuits

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

4.7.10.6 CE-100T-8 Card POS Ports History Window

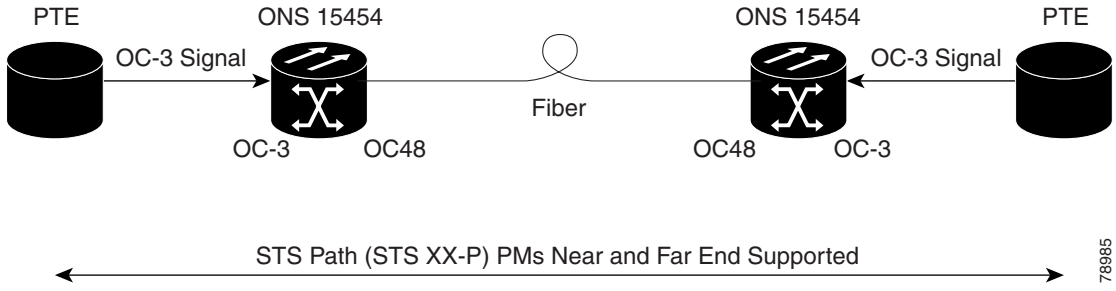
The Ethernet POS Ports History window lists past Ethernet POS Ports statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-21. The listed parameters are defined in Table 4-19 on page 4-31.

4.8 Performance Monitoring for Optical Cards

This section lists performance monitoring parameters for ONS 15454 optical cards, including the OC-3, OC-12, OC-48, and OC-192.

Figure 4-17 shows the signal types that support near-end and far-end PMs.

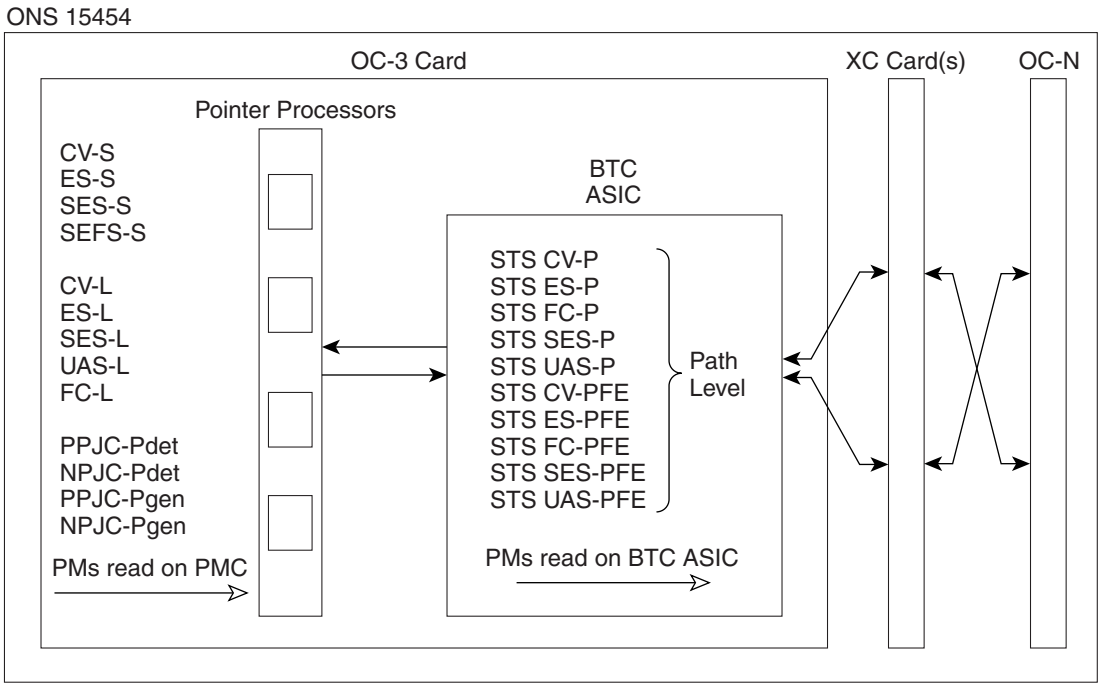
Figure 4-17 Monitored Signal Types for the OC-3 Cards



Note The XX in Figure 4-17 represents all PMs listed in Table 4-23, Table 4-24, and Table 4-25 with the given prefix and/or suffix.

Figure 4-18 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC3 IR 4 SH 1310 and OC3 IR SH 1310-8 cards.

Figure 4-18 PM Read Points on the OC-3 Cards



Note For PM locations relating to protection switch counts, see the Telcordia GR-253-CORE document.

Table 4-23 and Table 4-24 list the PM parameters for OC-3 cards.

Table 4-23 OC3 Card PMs

Section (NE)	Line (NE)	STS Path (NE)	Line (FE)	STS Path (FE)[1]
CV-S ES-S SES-S SEFS	CV-L ES-L SES-L UAS-L FC-L PSC (1+1) PSD (1+1)	CV-P ES-P SES-P UA-S-P FCP PPJC-PDET NPJC-PDET PPJC-PGEN NPJC-PGEN PPJC-SEC NPJC-SEC PJC-DIFF	CV-LFE ES-LFE SES-LFE UAS-LFE FC-LFE	CV-PFE ES-PFE SES-PFE UAS-PFE FC-PFE

1. The STS Path (FE) PMs are valid only for the OC3-4 card on ONS 15454.

Table 4-24 OC3-8 Card PMs

Section (NE)	Line (NE)	Physical Layer (NE)	STS Path (NE)	Line (FE)	STS Path (FE)
CV-S ES-S SES-S SEFS	CV-L ES-L SES-L UAS-L FC-L PSC (1+1) PSD (1+1)	LBCL OPT OPR	CV-P ES-P SES-P UAS-P FC-P PPJC-PDET NPJC-PDET PPJC-PGEN NPJC-PGEN PPJC-SEC NPJC-SEC PJC-DIFF	CV-LFE ES-LFE SES-LFE UAS-LFE FC-LFE	CV-PFE ES-PFE SES-PFE UAS-PFE FC-PFE

Table 4-25 lists the PM parameters for OC-12, OC-48, and OC-192 cards.

Table 4-25 OC12, OC48, OC192 Card PMs

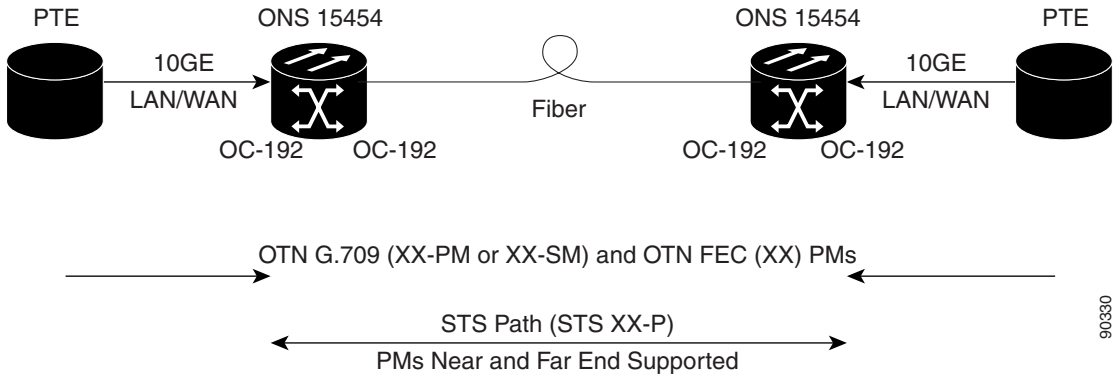
Section (NE)	Line (NE)	STS Path (NE)	Line (FE)
CV-S	CV-L	CV--P	CV-LFE
ES-S	ES-L	ESP	ES-LFE
SES-S	SES-L	SES-P	SES-LFE
SEFS	UAS-L	UAS-P	UAS-LFE
	FC-L	FC-P	FC-LFE
	PSC (1+1, 2F BLSR)	PPJC-PDET	
	PSD (1+1, 2F BLSR)	NPJC-PDET	
	PSC-W (4F BLSR)	PPJC-PGEN	
	PSD-W (4F BLSR)	NPJC-PGEN	
	PSC-S (4F BLSR)	PPJC-SEC	
	PSD-S (4F BLSR)	NPJC-SEC	
	PSC-R (4F BLSR)	PJC-DIFF	
	PSD-R (4F BLSR)		

4.9 Performance Monitoring for Transponder and Muxponder Cards

This section lists performance monitoring parameters for transponder cards (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_10E), and muxponder cards (MXP_2.5G_10G, MXP_25G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G).

Figure 4-19 shows the signal types that support near-end and far-end PMs.

Figure 4-19 Monitored Signal Types



Note The XX in Figure 4-19 represents all PMs listed in Table 4-26 with the given prefix and/or suffix.

Figure 4-20 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the TXP_MR_10G card.

Figure 4-20 PM Read Points

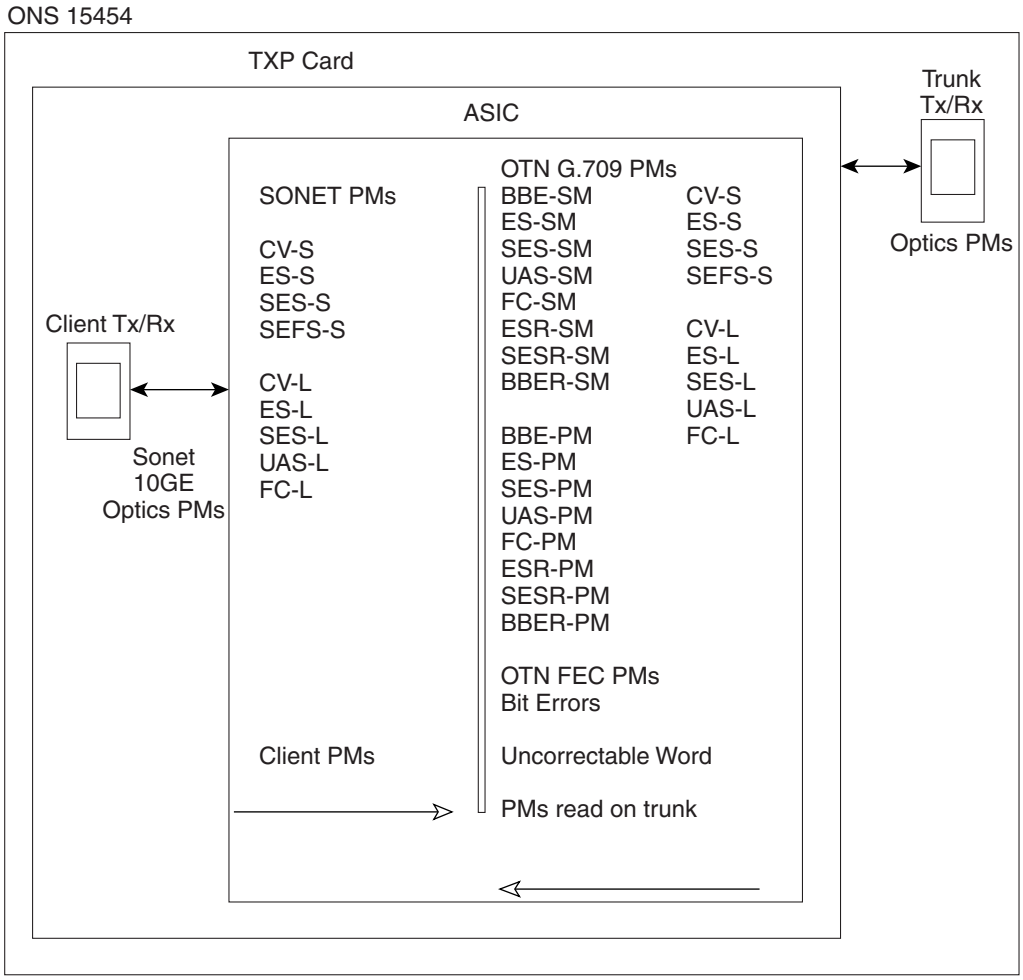


Table 4-26 describes the PM parameters for the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G cards.

Table 4-26 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10E Card PMs

SONET Layer Far-End (FE)[1]	SONET Layer Near-End (NE)[1]	OTN Layer (NE and FE)[2]	Optics (NE)[1, 3]	8B10B (NE)[4]	FEC (NE)[2]
CV-LFE	CV-S	ES-PM	OPT-AVG	CGV	BIEC
ES-LFE	CV-L	ES-SM	OPT-MAX	DCG	UNC-WORDS
SES-LFE	ES-S	ESR-PM	OPT-MIN	IOS	
UAS-LFE	ES-L	ESR-SM	OPR-AVG	IPC	
FC-LFE	SES-S	SES-PM	OPR-MAX	NIOS	
	SES-L	SES-SM	OPR-MIN	VPC	
	SEF-S	SESR-PM	LBCL-AVG		
	UAS-L	SESR-SM	LBCL-MAX		
	FC-L	UAS-PM			
		UAS-SM			
		BBE-PM			
		BBE-SM			
		BBER-PM			
		BBER-SM			
		FC-PM			
		FC-SM			

1. Applicable to OCH and CLNT facilities.
2. Applicable to OCH facility.
3. TXP-MR-2.5G/TXPP-MR-2.5G ESCON payload does not support optics PMs on the client port due to SFP imposed restriction.
4. Applicable to TXP_MR_2.5G and TXPP_MR_2.5G cards only.

4.9.1 MXP_MR_2.5G/MXPP_MR_2.5G Payload Statistics Window

The Payload Statistics window lists parameters at the line level. The Payload Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The Clear button sets the values on the card to zero. All counters on the card are cleared.

Table 4-27 defines the MXP_MR_2.5G/MXPP_MR_2.5G card statistical parameters.

Table 4-27 MXP_MR_2.5G/MXPP_MR_2.5G Statistical PMs

Parameter	Definition
8b/10b Errors	A count of 10b errors received by the serial/deserializer (serdes 8b/10b).
Running Disparity Count	A count of errors that affect the disparity of the received data stream.
Invalid CRC Error	A count of invalid cyclical redundancy checks.
Rx Frames	A count of the number of frames received without errors.
Tx Frames	A count of the number of transmitted frames.

Table 4-27 MXP_MR_2.5G/MXPP_MR_2.5G Statistical PMs (continued)

Parameter	Definition
Tx Bytes	A count of the number of bytes transmitted from the frame since the last counter reset.
Rx Link Reset (Only for FC Mode)	A count of the received link resets.

4.9.2 MXP_MR_2.5G/MXPP_MR_2.5G Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments.

The **Utilization** window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps). The maxBaseRate for MXP_MR_2.5G/MXPP_MR_2.5G cards is shown in Table 4-28.

Table 4-28 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

4.9.3 MXP_MR_2.5G/MXPP_MR_2.5G History Window

The MXP_MR_2.5G/MXPP_MR_2.5G History window lists past statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-29. The listed parameters are defined in Table 4-27 on page 4-39.

Table 4-29 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals

Table 4-29 Ethernet History Statistics per Time Interval (continued)

Time Interval	Number of Intervals Displayed
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

4.10 Performance Monitoring for Storage Media Access Cards

The following sections define performance monitoring parameters and definitions for storage media card, also known as the FC-MR-4 or Fibre Channel card.

CTC provides FC_MR-4 performance information, including line-level parameters, port bandwidth consumption, and historical statistics. The FC_MR-4 card performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

4.10.1 FC_MR-4 Statistics Window

The Statistics window lists parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared.

Table 4-30 defines the FC_MR-4 card Statistics parameters.

Table 4-30 FC_MR-4 Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Fibre Channel link is receiving a valid Fibre Channel signal (carrier) from the attached Fibre Channel device; up means present, and down means not present.
Rx Frames	A count of the number of Fibre Channel frames received without errors.
Rx Bytes	A count of the number of bytes received without error for the Fibre Channel payload.
Tx Frames	A count of the number of transmitted Fibre Channel frames.
Tx Bytes	A count of the number of bytes transmitted from the Fibre Channel frame.
8b/10b Errors	A count of 10b errors received by the serial/deserializer (serdes 8b/10b).
Encoding Disparity Errors	A count of the disparity errors received by serdes.
Link Recoveries	A count of the FC_MR-4 software initiated link recovery attempts toward the FC line side because of SONET protection switches.
Rx Frames bad CRC	A count of the received Fibre Channel frames with errored CRCs.
Tx Frames bad CRC	A count of the transmitted Fibre Channel frames with errored CRCs.

Table 4-30 FC_MR-4 Statistics Parameters (continued)

Parameter	Definition
Rx Undersized Frames	A count of the received Fibre Channel frames < 36 bytes including CRC, start of frame (SOF), and end of frame (EOF).
Rx Oversized Frames	A count of the received Fibre Channel frames > 2116 bytes of the payload. Four bytes are allowed for supporting VSAN tags sent.
GFP Rx HDR Single-bit Errors	A count of generic framing procedure (GFP) single bit errors in the core header error check (CHEC).
GFP Rx HDR Multi-bit Errors	A count of GFP multibit errors in the CHEC.
GGFP Rx Frames Invalid Type	A count of GFP invalid user payload identifier (UPI) field in the type field.
GFP Rx Superblk CRC Errors	A count of superblock CRC errors in the transparent GFP frame.

4.10.2 FC_MR-4 Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments. The **Utilization** window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 24) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 24) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps or 2 Gbps). The maxBaseRate for FC_MR-4 cards is shown in Table 4-31.

Table 4-31 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-24	850000000
STS-48	850000000 x 2[1]

1. For 1 Gbps of bit rate being transported, there are only 850 Mbps of actual data because of 8b->10b conversion. Similarly, for 2 Gbps of bit rate being transported there are only 850 Mbps x 2 of actual data.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

4.10.3 FC_MR-4 History Window

The History window lists past FC_MR-4 statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 4-32. The listed parameters are defined in Table 4-30 on page 4-41.

Table 4-32 FC_MR-4 History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

4.11 Performance Monitoring for DWDM Cards

The following sections define performance monitoring parameters and definitions for the ONS 15454 OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, OSC-CSM, and 32WSSDWDM cards.

4.11.1 Optical Amplifier Card Performance Monitoring Parameters

The PM parameters for the OPT-PRE and OPT-BST cards are listed Table 4-33.

Table 4-33 Optical PM Parameters for OPT-PRE and OPT-BST Cards

Optical Line	Optical Amplifier Line
OPT	OPR

4.11.2 Multiplexer and Demultiplexer Card Performance Monitoring Parameters

The PM parameters for the 32MUX-O, 32WSS, 32DMX, and 32DMX-O cards are listed in Table 4-34.

Table 4-34 Optical PMs for 32MUX-O and 32DMX-O Cards

Optical Channel	Optical Line
OPR	OPT

4.11.3 4MD-xx.x Card Performance Monitoring Parameters

The PM parameters for the 4MD-xx.x cards are listed in Table 4-35.

Table 4-35 Optical PMs for 4MD-xx.x Cards

Optical Channel	Optical Band
OPR	OPT

4.11.4 OADM Channel Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x cards are listed in Table 4-36.

Table 4-36 Optical PMs for AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x Cards

Optical Channel	Optical Line
OPR	OPT

4.11.5 OADM Band Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1B-xx.x and AD-4B-xx.x cards are listed in Table 4-37.

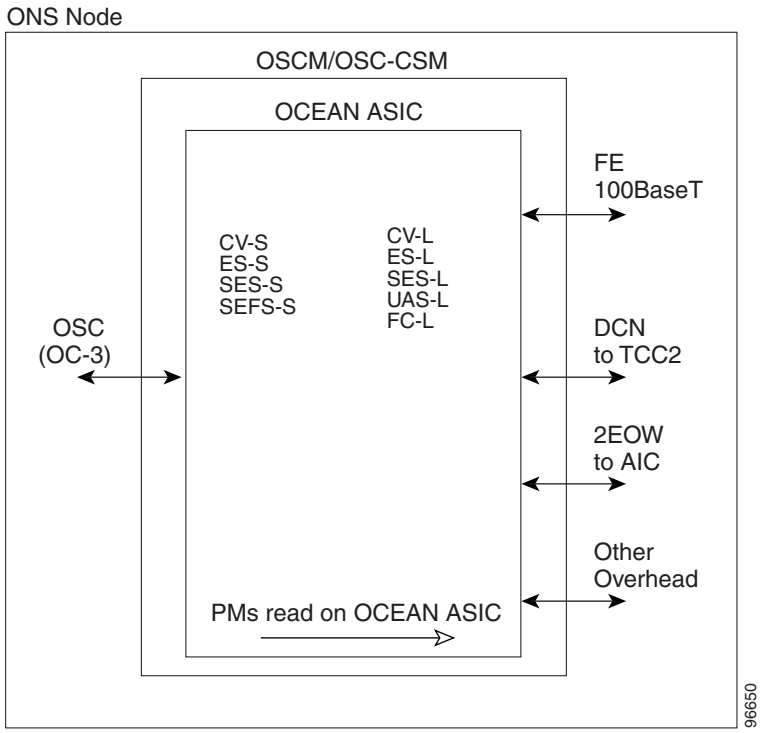
Table 4-37 Optical PMs for AD-1B-xx.x and AD-4B-xx.x Cards

Optical Line	Optical Band
OPR	OPT

4.11.6 Optical Service Channel Card Performance Monitoring Parameters

Figure 4-21 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OSCM and OSC-CSM cards.

Figure 4-21 PM Read Points on OSCM and OSC-CSM Cards



The PM parameters for the OSCM and OSC-CSM cards are described in Table 4-38.

Table 4-38 OSCM/OSC-CSM (OC3) Card PMs

Section (NE)[1]	Line (NE/FE)[1]	Optics (NE)[2]
CV-S ES-S SES-S SEF-S	CV-L ES-L SES-L UAS-L FC-L	OPWR

1. Applicable to OC3
2. Applicable to OTS facilities

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454.

For SNMP setup information, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Chapter topics include:

5.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15454 network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

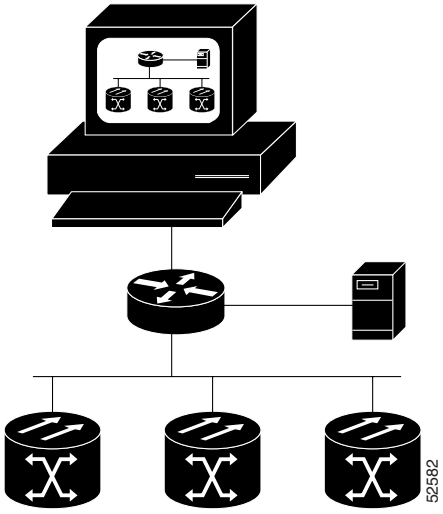
The ONS 15454 uses SNMP for asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both of these versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15454.

Note The CERENT-MSDWDM-MIB.mib and CERENT-FC-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. However, the respective SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

Figure 5-1 illustrates the basic layout idea of an SNMP-managed network.

Figure 5-1 Basic Network Managed by SNMP

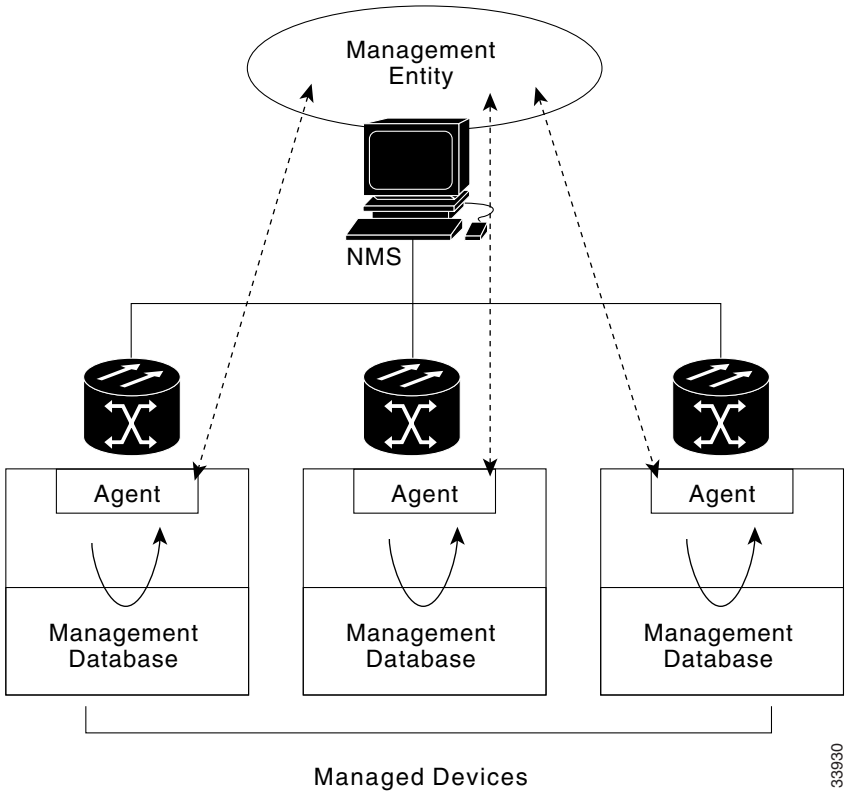


5.2 Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

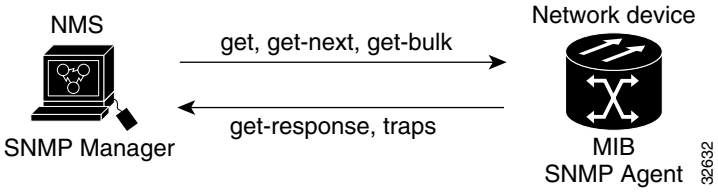
A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or more management systems. Figure 5-2 illustrates the relationship between the network manager, SNMP agent, and the managed devices.

Figure 5-2 Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. Figure 5-3 illustrates SNMP agent get-requests that transport data to the network management software.

Figure 5-3 Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from management information bases, or MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15454)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available via SNMP to other management systems having the same protocol compatibility.

5.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-part SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

5.4 SNMP Version Support

The ONS 15454 supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15454 SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SONET multiplexers using a supported MIB.

Note ONS 15454 MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains two 64-bit performance monitoring counters, CERENT-MSDWDM-MIB.mib and CERENT-FC-MIB.mib. The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

5.5 SNMP Version Support

The ONS 15454 supports SNMP v1 and SNMPv2c traps and get requests. The SNMP MIBs in the ONS 15454 define alarms, traps, and status. Through SNMP, NMS applications can query a management agent using a supported MIB. The functional entities include Ethernet switches and SONET multiplexers. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to set up or change SNMP settings.

5.6 SNMP Message Types

The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP messages. Table 5-1 describes these messages.

Table 5-1 ONS 15454 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.

Table 5-1 ONS 15454 SNMP Message Types (continued)

Operation	Description
set-request	Provides remote network monitoring (RMON) MIB.
trap	Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager.

5.7 SNMP Management Information Bases

Table 5-2 lists the IETF-standard MIBs implemented in the ONS 15454SNMP agents.

First compile the MIBs in the in Table 5-2. Compile the Table 5-3 MIBs next.

Caution If you do not compile MIBs in the correct order, one or more might not compile correctly.

Table 5-2 IETF Standard MIBs Implemented in the ONS 15454 System

RFC[1] Number	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213	RFC1213-MIB-rfc1213.mib	Management Information Base for Network
1907	SNMPV2-MIB-rfc1907.mib	Management of TCP/IP-based Internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	OSPF Version 2 Management Information Base
1493	BRIDGE-MIB-rfc1493.mib	Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network [LAN] segments.)
2819	RMON-MIB-rfc2819.mib	Remote Network Monitoring Management Information Base
2737	ENTITY-MIB-rfc2737.mib	Entity MIB (Version 2)
2233	IF-MIB-rfc2233.mib	Interfaces Group MIB using SMIv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS3/E3 Interface Type
2558	SONET-MIB-rfc2558.mib	Definitions of Managed Objects for the SONET/SDH Interface Type

Table 5-2 IETF Standard MIBs Implemented in the ONS 15454 System (continued)

RFC[1] Number	Module Name	Title/Comments
2674	P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
3273	HC-RMON-MIB	The MIB module for managing remote monitoring device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513 and RMON-2 MIB as specified in RFC 2021

1. RFC = Request for Comment

Each ONS system is shipped with a software CD containing applicable proprietary MIBs. Table 5-3 lists the proprietary MIBs for the ONS 15454.

Table 5-3 ONS 15454 Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib
4	CERENT-GENERIC.mib (not applicable to ONS 15454)
5	CISCO-SMI.mib
6	CISCO-VOA-MIB.mib
7	CERENT-MSDWDM-MIB.mib
8	CISCO-OPTICAL-MONITOR-MIB.mib
100	CERENT-FC-MIB.mib

Note If you cannot compile the proprietary MIBs correctly, log into the Technical Support Website at http://www.cisco.com/techsupport or call Cisco TAC (800) 553-2447.

Note When SNMP indicates that the wavelength is unknown, it means that the corresponding card (MXP_2.5G_10E, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) works with the first tunable wavelength.

5.8 SNMP Trap Content

The ONS 15454 generates all alarms and events, such as raises and clears, as SNMP traps. These contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; synchronous transport signal [STS] and Virtual Tributary [VT]; bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], etc.).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service affecting).
- Date and time stamp showing when the alarm occurred.

5.8.1 Generic and IETF Traps

The ONS 15454 supports the generic IETF traps listed in Table 5-4.

Table 5-4 ONS 15454 Traps

Trap	From RFC No. MIB	Description
coldStart	RFC1907-MIB	Agent up, cold start.
warmStart	RFC1907-MIB	Agent up, warm start.
authenticationFailure	RFC1907-MIB	Community string does not match.
newRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree.
topologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking.
entConfigChange	RFC2737/ ENTITY-MIB	The entLastChangeTime value has changed.
dsx1LineStatusChange	RFC2495/ DS1-MIB	The value of an instance of dsx1LineStatus has changed. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (for example, a DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	The value of an instance of dsx3LineStatus has changed. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (for example, a DS-1), no traps for the lower-level are sent.
risingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

5.8.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. ONS 15454 traps and variable bindings are listed in Table 5-5. For each group (such as Group A), all traps within the group are associated with all of its variable bindings.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
A	dsx1LineStatusChange (from RFC 2495)	(1)	dsx1LineStatus	This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information.
		(2)	dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent re-initialization, the value of this object is zero.
		(3)	cerent454NodeTime	The time that an event occurred.
		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.
B	dsx3LineStatusChange (from RFC 2496)	(1)	dsx3LineStatus	This variable indicates the line status of the interface. It contains loopback state information and failure state information.
		(2)	dsx3LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then the value is zero.
		(3)	cerent454NodeTime	The time that an event occurred.
		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
C	coldStart (from RFC 1907)	(1)	cerent454NodeTime	The time that the event occurred.
	warmStart (from RFC 1907)	(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
	newRoot (from RFC)	(3)	snmpTrapAddress	The address of the SNMP trap.
	topologyChange (from RFC)		—	—
	entConfigChange (from RFC 2737)		—	—
	authenticationFailure (from RFC 1907)		—	—
D1	risingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmRisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is greater than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.
		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
D2	fallingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmFallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single is also generated if the first sample after this entry is less than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.
		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
E	failureDetectedExternal ToTheNE (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerent454AlarmAdditionalInfo	Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero.
		(10)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
F	performanceMonitorThresholdCrossingAlert (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerent454ThresholdMonitorType	This object indicates the type of metric being monitored.
		(10)	cerent454ThresholdLocation	Indicates whether the event occurred at the near- or far end.
		(11)	cerent454ThresholdPeriod	Indicates the sampling interval period.
		(12)	cerent454*ThresholdSetValue*	The value of this object is the threshold provisioned by the NMS.
		(13)	cerent454ThresholdCurrentValue	
		(14)	cerent454ThresholdDetectType	
		(15)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
G	All other traps (from CERENT-454-MIB) not listed above	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	snmpTrapAddress	The address of the SNMP trap.

5.9 SNMP Community Names

Community names are used to group SNMP trap destinations. All ONS 15454 trap destinations can be provisioned as part of SNMP communities in Cisco Transport Controller (CTC). When community names are assigned to traps, the ONS 15454 treats the request as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.

5.10 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or from outside networks. Release 5.0 (and 4.6.x) versions of CTC enable network operations centers (NOCs) to access performance monitoring data such as remote monitoring (RMON) statistics or autonomous messages across firewalls by using an SMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy is intended for use in a gateway network element-end network element (GNE-ENE) topology with many NEs through a single NE gateway. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls. The proxy interoperates with common NMS such as HP-OpenView.

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15454 Procedure Guide*.

5.11 Remote Monitoring

The ONS 15454 incorporates RMON to allow network operators to monitor Ethernet card performance and events. (The ONS 15600 does not support RMON.) The RMON thresholds are user-provisionable in CTC. Refer to the *Cisco ONS 15454 Procedure Guide for instructions*. Note that otherwise, RMON operation is invisible to the typical CTC user.

ONS 15454 system RMON implementation is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

5.11.1 HC-RMON-MIB Support

For the ONS 15454, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for this support. All of these elements are accessible by any third-party SNMP client having RFC 3273 support.

5.11.2 Ethernet Statistics RMON Group

The Ethernet Statistics group contains the basic statistics monitored for each subnetwork in a single table called the etherStatsTable.

5.11.2.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note EtherStatsTable entries are not preserved if the SNMP agent is restarted.

5.11.2.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15454 Ethernet cards.

5.11.2.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus “invalid” value (4). The OID marks the row for deletion. If required, a deleted row can be recreated.

5.11.2.4 64-Bit etherStatsHighCapacity Table

The Ethernet statistics group contains 64-bit statistics in the etherStatsHighCapacityTable, which provides 64-bit RMON support for the HC-RMON-MIB. The etherStatsHighCapacityTable is an extension of the etherStatsTable that adds 16 new columns for performance monitoring data in 64-bit format. There is a one-to-one relationship between the etherStatsTable and etherStatsHighCapacityTable when rows are created or deleted in either table.

5.11.3 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

5.11.3.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 5-6 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods. For example, an ONS 15454 E100 card contains 24 ports, which multiplied by periods allows 96 rows in the table. An E1000 card contains 14 ports, which multiplied by four periods allows 56 table rows.

Table 5-6 RMON History Control Periods and History Categories

Sampling Periods (historyControlValue Variable)	Total Values, or Buckets (historyControl Variable)
15 minutes	32
24 hours	7
1 minute	60
60 minutes	24

5.11.3.2 Row Creation in historyControlTable

The SetRequest PDU must be able to activate a historyControlTable row in one single-set operation. In order to do this, the PDU must contain all needed values and have a status variable value of 2 (createRequest). All OIDs in the SetRequest PDU should be type OID.0 type for entry creation.

To create a creation SetRequest PDU for the historyControlTable, the following values are required:

- The historyControlDataSource and its desired value
- The historyControlBucketsRequested and it desired value
- The historyControlInterval and its desired value
- The historyControlOwner and its desired value
- The historyControlStatus with a value of createRequest (2)

The historyControlBucketsRequested OID value is ignored because the number of buckets allowed for each sampling period, based upon the historyControlInterval value, is already fixed as listed in Table 5-6.

The historyControlInterval value cannot be changed from the four allowed choices. If you use another value, the SNMP agent selects the closest smaller time period from the set buckets. For example, if the set request specifies a 25-minute interval, this falls between the 15-minute (32 bucket) variable and the 60-minute (24 bucket) variable. The SNMP agent automatically selects the lower, closer value, which is 15 minutes, so it allows 32 buckets.

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

5.11.3.3 Get Requests and GetNext Requests

These PDUs are not restricted.

5.11.3.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

5.11.4 Ethernet History RMON Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

5.11.4.1 64-Bit etherHistoryHighCapacityTable

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

5.11.5 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

5.11.5.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

5.11.5.2 Row Creation in alarmTable

To create a row in the alarmTable, the SetRequest PDU must be able to create the row in one single-set operation. All OIDs in the SetRequest PDU should be type OID.0 type for entry creation. The table has a maximum number of 256 rows.

To create a creation SetRequest PDU for the alarmTable, the following values are required:

- The alarmInterval and its desired value
- The alarmVariable and its desired value
- The alarmSampleType and its desired value
- The alarmStartupAlarm and its desired value
- The alarmOwner and its desired value
- The alarmStatus with a value of createRequest (2)

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

In addition to the required values, the following restrictions must be met in the SetRequest PDU:

- The alarmOwner is a string of length 32 characters.
- The alarmRisingEventIndex always takes value 1.
- The alarmFallingEventIndex always takes value 2.
- The alarmStatus has only two values supported in SETs: createRequest (2) and invalid (4).
- The AlarmVariable is of the type OID.ifIndex, where ifIndex gives the interface this alarm is created on and OID is one of the OIDs supported in Table 5-7.

Table 5-7 OIDs Supported in the AlarmTable

No.	Column Name	OID	Status
1	ifInOctets	{1.3.6.1.2.1.2.2.1.10}	—
2	IfInUcastPkts	{1.3.6.1.2.1.2.2.1.11}	—
3	ifInMulticastPkts	{1.3.6.1.2.1.31.1.1.1.2}	Unsupported in E100/E1000
4	ifInBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.3}	Unsupported in E100/E1000
5	ifInDiscards	{1.3.6.1.2.1.2.2.1.13}	Unsupported in E100/E1000
6	ifInErrors	{1.3.6.1.2.1.2.2.1.14}	—
7	ifOutOctets	{1.3.6.1.2.1.2.2.1.16}	—
8	ifOutUcastPkts	{1.3.6.1.2.1.2.2.1.17}	—
9	ifOutMulticastPkts	{1.3.6.1.2.1.31.1.1.1.4}	Unsupported in E100/E1000
10	ifOutBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.5}	Unsupported in E100/E1000
11	ifOutDiscards	{1.3.6.1.2.1.2.2.1.19}	Unsupported in E100/E1000
12	Dot3StatsAlignmentErrors	{1.3.6.1.2.1.10.7.2.1.2}	—
13	Dot3StatsFCSErrors	{1.3.6.1.2.1.10.7.2.1.3}	—
14	Dot3StatsSingleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.4}	—
15	Dot3StatsMultipleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.5}	—
16	Dot3StatsDeferredTransmissions	{1.3.6.1.2.1.10.7.2.1.7}	—
17	Dot3StatsLateCollisions	{1.3.6.1.2.1.10.7.2.1.8}	—
18	Dot3StatsExcessiveCollisions	{13.6.1.2.1.10.7.2.1.9}	—
19	Dot3StatsFrameTooLong	{1.3.6.1.2.1.10.7.2.1.13}	—
20	Dot3StatsCarrierSenseErrors	{1.3.6.1.2.1.10.7.2.1.11}	Unsupported in E100/E1000
21	Dot3StatsSQETestErrors	{1.3.6.1.2.1.10.7.2.1.6}	Unsupported in E100/E1000
22	etherStatsUndersizePkts	{1.3.6.1.2.1.16.1.1.1.9}	—
23	etherStatsFragments	{1.3.6.1.2.1.16.1.1.1.11}	—
24	etherStatsPkts64Octets	{1.3.6.1.2.1.16.1.1.1.14}	—
25	etherStatsPkts65to127Octets	{1.3.6.1.2.1.16.1.1.1.15}	—
26	etherStatsPkts128to255Octets	{1.3.6.1.2.1.16.1.1.1.16}	—
27	etherStatsPkts256to511Octets	{1.3.6.1.2.1.16.1.1.1.17}	—
28	etherStatsPkts512to1023Octets	{1.3.6.1.2.1.16.1.1.1.18}	—
29	etherStatsPkts1024to1518Octets	{1.3.6.1.2.1.16.1.1.1.19}	—
30	EtherStatsBroadcastPkts	{1.3.6.1.2.1.16.1.1.1.6}	—
31	EtherStatsMulticastPkts	{1.3.6.1.2.1.16.1.1.1.7}	—
32	EtherStatsOversizePkts	{1.3.6.1.2.1.16.1.1.1.10}	—
33	EtherStatsJabbers	{1.3.6.1.2.1.16.1.1.1.12}	—
34	EtherStatsOctets	{1.3.6.1.2.1.16.1.1.1.4}	—
35	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.13}	—

Table 5-7 OIDs Supported in the AlarmTable (continued)

No.	Column Name	OID	Status
36	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.8}	—
37	EtherStatsDropEvents	{1.3.6.1.2.1.16.1.1.1.3}	Unsupported in E100/E1000 and G1000

5.11.5.3 Get Requests and GetNext Requests

These PDUs are not restricted.

5.11.5.4 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

5.11.6 Event RMON Group

The Event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15454 implements the logTable as specified in RFC 2819.

5.11.6.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always log-and-trap (4).
- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be despatched to all provisioned destinations.
- The eventOwner column value is always “monitor.”
- The eventStatus column value is always valid(1).

5.11.6.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.