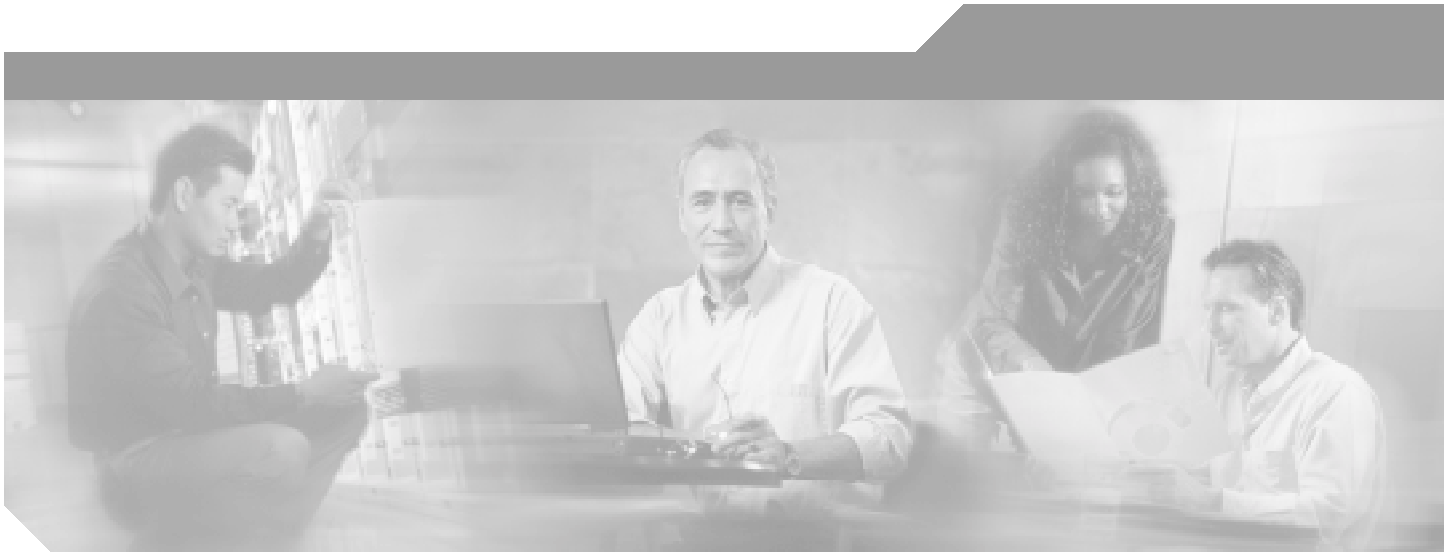


Cisco ONS 15327 Troubleshooting Guide

Product and Documentation Release 3.4
April 2003

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-7815641=
Text Part Number: 78-15641-01

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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)

Cisco ONS 15327 Troubleshooting Guide
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

CONTENTS

FIGURES

TABLES

About this Guide

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

This section provides the following information:

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

Document Objectives

The *Cisco ONS 15327 Troubleshooting Guide* provides troubleshooting procedures for SONET alarms and error messages and provides symptoms and solutions for general troubleshooting problems with CTC and hardware. This guide also contains hardware replacement procedures. Use this document 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.

Related Documentation

Use this *Cisco ONS 15327 Troubleshooting Guide* in conjunction with the following referenced publications:

- *Cisco ONS 15327 Procedure Guide, Release 3.4*
  Provides installation, turn up, provisioning, and maintainence procedures for Cisco ONS 15327 nodes and networks
- *Cisco ONS 15327 Reference Manual, Release 3.4*
  Provides reference information including detailed card specifications, feature descriptions, and topology information
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.4*
  Provides a comprehensive list of TL1 commands for the ONS 15327 and ONS 15454
- *Release Notes for the Cisco ONS 15327 Release 3.4*
  Provides up-to-date caveats, closed issues, and new feature information

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. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco ONS 15327 Installation Handbook* that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15327. It also includes translations of the safety warnings that appear in the ONS 15327 system documentation.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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 Networking Products MarketPlace:

  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, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15327. To troubleshoot specific ONS 15327 alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for contact the Cisco Technical Assistance Center (Cisco TAC).

This chapter includes the following sections on network problems:

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

Note For network acceptance tests, refer to the *Cisco ONS 15327 Procedure Guide*.

- 1.2 Identify Points of Failure on a DS-N Circuit Path—Describes the steps to perform loopback and hairpin tests, which you can use to test DS-N circuit paths through the network or logically isolate faults.
- 1.3 Identify Points of Failure on an OC-N Circuit Path—Describes the steps to perform loopback and hairpin tests, which you can use to test OC-N circuit paths through the network or logically isolate faults.

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

- 1.4 Restoring the Database and Default Settings—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.5 PC Connectivity Troubleshooting—Provides troubleshooting procedures for PC and network connectivity to the ONS 15327.
- 1.6 CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC login or operation problems.
- 1.7 Circuits and Timing—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- 1.8 Fiber and Cabling—Provides troubleshooting procedures for fiber and cabling connectivity errors.

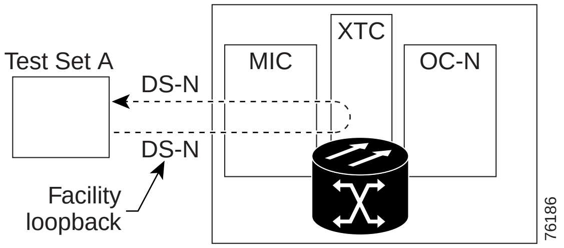
1.1 Network Troubleshooting Tests

Use loopbacks and hairpins to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15327 line (traffic) cards, except Ethernet cards, allow loopbacks and hairpins.

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

A facility loopback tests the line interface unit (LIU) of a card, the mechanical interface card (MIC), 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 MIC, or the cabling plant as the potential cause of a network problem. Figure 1-1 shows a facility loopback on an XTC-14 or XTC-28-3 card.

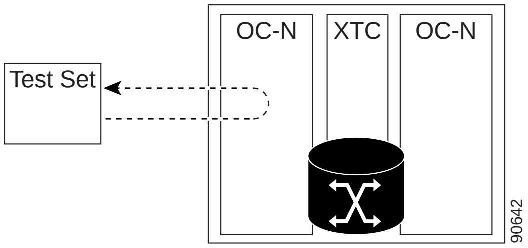
Figure 1-1 Facility Loopback Process on an XTC Card



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

Caution Before performing a facility loopback on an OC-N card, make sure the card contains at least two data communications channel (DCC) paths to the node where the card is installed. A second DCC provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15327 containing the loopback OC-N card.

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



A terminal loopback tests a circuit path as it passes through the XTC card and loops back from the card with the loopback. Figure 1-3 on page 1-3 shows a terminal loopback on an OC-N card. The test-set traffic comes in on the MIC card DS-N ports and goes through the XTC card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it back through the XTC card to the MIC card. This test verifies that the XTC card cross-connect circuit paths are valid, but does not test the LIU on the OC-N card.

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

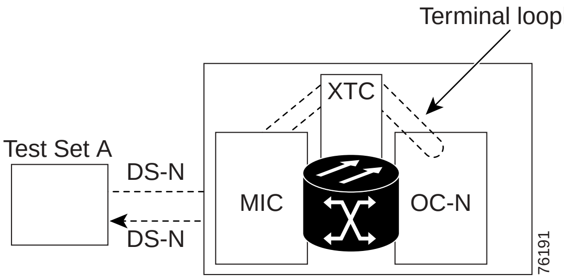
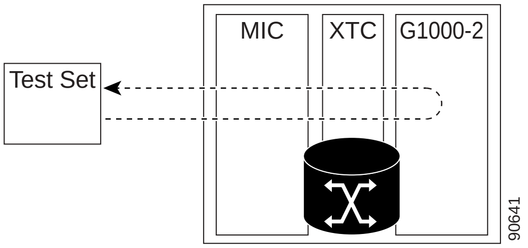


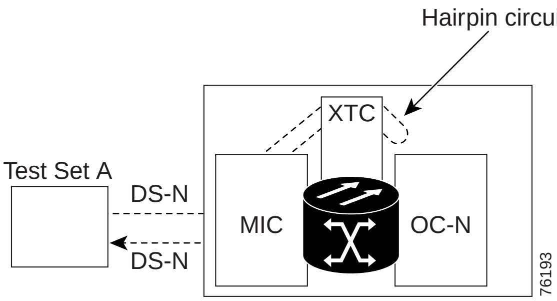
Figure 1-4 shows a terminal loopback on a G1000-2 card. The test-set traffic comes in on the MIC card DS-N ports and goes through the XTC card to the G1000-2 card. The terminal loopback on the G1000-2 card turns the signal around before it reaches the LIU and sends it back through the XTC card to the MIC card. This test verifies that the XTC card cross-connect circuit paths are valid, but does not test the LIU on the G1000-2 card.

Figure 1-4 Terminal Loopback Process on a G1000-2 Card



A hairpin circuit brings traffic in and out on a DS-N port instead of sending the traffic onto the OC-N. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, which would drop all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic. Figure 1-5 shows the hairpin circuit process on a OC-N card.

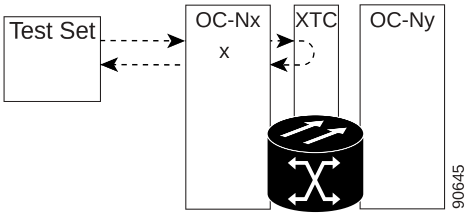
Figure 1-5 Hairpin Circuit Process on an OC-N Card



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

You can create a cross-connect loopback on all working or protect optical ports unless the protect port is used in a 1+1 protection group and is in working mode. If a terminal or facility loopback exists on a port, you cannot use the cross-connect loopback. Figure 1-6 shows a cross-connect loopback on an OC-N port.

Figure 1-6 Cross-Connect Loopback Process on an OC-N Port



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

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

The example in this section tests an DS-N circuit on a two-node bidirectional line switched ring (BLSR). Using a series of facility loopbacks, hairpin circuits, and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of network test procedures applies to this scenario:

1. Facility loopback on the source-node XTC port
2. Hairpin on the source-node XTC port
3. Terminal loopback to the destination-node XTC port
4. Hairpin on the destination-node XTC port
5. Facility loopback to the destination XTC port

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

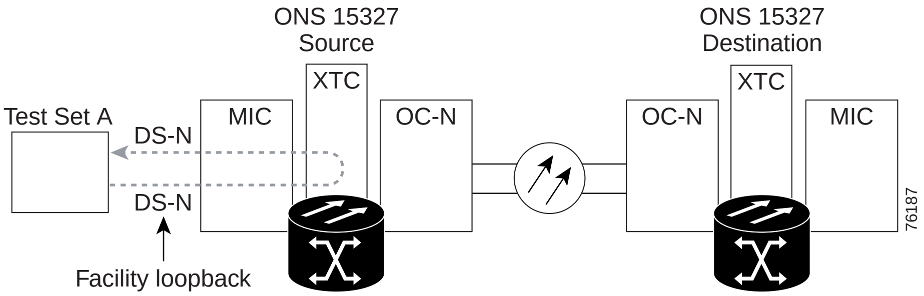
Note All loopback tests require on-site personnel.

Note These procedures are performed when power connections to the node(s) or site(s) are assumed to be within necessary specifications. If the network tests do not isolate the problems, troubleshoot outward for power failure.

1.2.1 Perform a Facility Loopback on a Source XTC Port

The facility loopback test is performed on the node source port in the network circuit; in this example, the test is routed through the MIC card and performed on the XTC port in the source node. Completing a successful facility loopback on this port isolates the cabling, MIC card, and XTC card as possible failure points. Figure 1-7 shows an example of a facility loopback on a source node XTC port.

Figure 1-7 Facility Loopback on a Source XTC Port



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

Note Loopbacks operate only on ports in the out of service-maintenance (OOS_MT) state.

Procedure: Create the Facility Loopback on the Source XTC Port

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

Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the MIC card, which interfaces with the XTC card. Both Tx and Rx connect to the same port. Adjust the test set accordingly.

Step 2 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

c. Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.

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

e. Click the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

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

Step 3 Proceed to the "Test the Facility Loopback" procedure on page 1-6.

Procedure: Test the Facility Loopback

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

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

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

a. Clear the loopback:

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

b. Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-23.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card, faulty XTC card, or faulty cabling from the DS-N port.

Step 5 Proceed to the "Test the DS-N Cabling" procedure on page 1-6.

Procedure: Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC ports) with a cable known to be good.

If a cable known to be good is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test-set traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

a. Replace the defective cable.

b. Clear the loopback:

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

- **c.** Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-23.

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

Step 5 Proceed to the "Test the XTC Card" procedure on page 1-7.

Procedure: Test the XTC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably a defective card:

- **a.** Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.
- **b.** Replace the faulty card.
- **c.** Clear the loopback:
  - Click the **Maintenance** > **Loopback** tabs.
  - Choose **None** from the Loopback Type column for the port being tested.
  - Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
  - Click the **Apply** button.
  - Click the **Yes** button in the Confirmation Dialog box.
- **d.** Proceed to the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-8.

Step 4 If the test set indicates a fault circuit, the problem might be faulty cabling from the MIC card to the XTC card or a faulty MIC card.

Step 5 Proceed to the "Test the MIC Cabling" procedure on page 1-7.

Procedure: Test the MIC Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC or from the MIC to the XTC) with a cable that is known to be good.

If a good cable is not available, test the suspect cable with a test set. Remove the suspect cable and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Resend test traffic on the loopback circuit with a cable that is known to be good installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

- **a.** Replace the defective cable.

b. Clear the facility loopback:

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

c. Proceed to the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-8.

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

Step 5 Proceed to the "Test the MIC Card" procedure on page 1-8.

Procedure: Test the MIC Card

Step 1 Replace the suspect card with a good card. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably a defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the loopback:

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

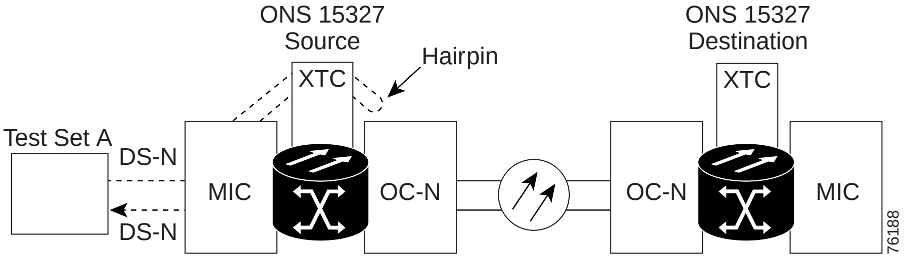
Step 4 If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 5 Proceed to the "1.2.2 Perform a Hairpin on a Source Node XTC Port" section on page 1-8.

1.2.2 Perform a Hairpin on a Source Node XTC Port

The hairpin test is performed on the first XTC card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through this card isolates the possibility that the source XTC card is the cause of the faulty circuit. Figure 1-8 on page 1-9 shows an example of a hairpin circuit on a source node XTC port.

Figure 1-8 Hairpin Circuit on a Source Node XTC Port



Note An XTC card is required to operate the ONS 15327 and can be used in a redundant or nonredundant configuration.

Procedure: Create the Hairpin on the Source Node Port

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

- If you just completed the "Perform a Facility Loopback on a Source XTC Port" procedure on page 1-5, leave the electrical test set hooked up to the MIC port.
- If you are starting the current procedure without the electrical test set hooked up to the MIC port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the MIC connectors for the port you are testing. The Tx and Rx terminals connect to the same port.

Adjust the test set accordingly.

Step 2 Use CTC to set up the hairpin on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the circuit **Type** and **Size** to the normal preferences.

d. Uncheck the **Bidirectional** check box and click the **Next** button.

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

f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.

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

Step 4 Proceed to the "Test the Hairpin Circuit" procedure on page 1-9.

Procedure: Test the Hairpin Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin loopback circuit:

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Terminal Loopback on a Destination XTC Port" procedure on page 1-11.

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

Step 5 Proceed to the "Test the Alternate Source XTC Card" procedure on page 1-10.

Procedure: Test the Alternate Source XTC Card

Step 1 Perform a reset on the active XTC card:

a. Determine the active XTC card. On both the physical node and the Cisco Transport Controller (CTC) window, the active XTC card has a green ACT LED, and the standby XTC card has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby XTC displays a green ACT LED.
- The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
- The LEDs should complete this sequence within 5 to 10 minutes.

Step 2 Resend test traffic on the loopback circuit. The test-set traffic now travels through the alternate XTC card.

Step 3 If the test set indicates a faulty circuit, assume that the XTC card is not causing the problem:

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Terminal Loopback on a Destination XTC Port" procedure on page 1-11.

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

Step 5 To confirm a defective original XTC card, proceed to the "Retest the Original Source XTC Card" procedure on page 1-11.

Procedure: Retest the Original Source XTC Card

Step 1 Perform a side switch of the XTC cards to make the original card the active card.

Step 2 Resend test-set traffic on the loopback circuit.

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

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective XTC card. See Chapter 3, "Replace Hardware" for details.

c. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the original XTC card might have had a temporary problem that is cleared by the side switch.

Clear the hairpin circuit:

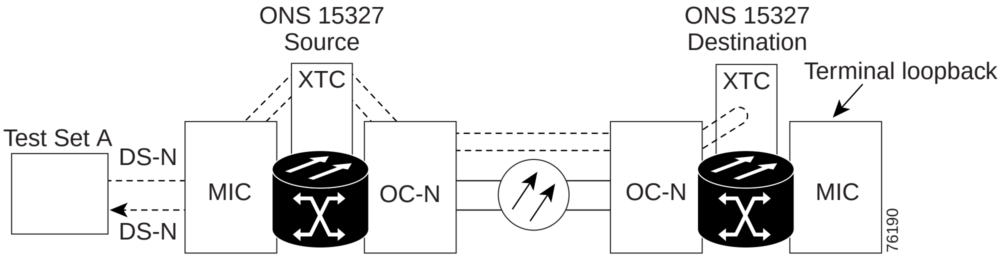
- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 5 Proceed to the "1.2.3 Perform a Terminal Loopback on a Destination XTC Port" section on page 1-11.

1.2.3 Perform a Terminal Loopback on a Destination XTC Port

The terminal loopback test is performed on the node destination port in the circuit; in this example, the XTC port in the destination node. First, create a bidirectional circuit that starts on the source node DS-N port and terminates on the destination node DS-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a destination node XTC port verifies that the circuit is good up to the destination XTC. Figure 1-9 on page 1-12 shows an example of a terminal loopback on a destination node XTC port.

Figure 1-9 Terminal Loopback on a Destination XTC Port



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

Procedure: Create the Terminal Loopback on a Destination XTC Port

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

- **a.** If you just completed the "Perform a Hairpin on a Source Node XTC Port" procedure on page 1-8, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the MIC card, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the MIC connectors for the port you are testing. The Tx and Rx connect to the same port.
- **c.** Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

- **a.** Click the **Circuits** tab and click the **Create** button.
- **b.** Give the circuit an easily identifiable name, such as DSNtoDSN.
- **c.** Set circuit **Type** and **Size** to the normal preferences.
- **d.** Leave the **Bidirectional** check box checked and click the **Next** button.
- **e.** In the Circuit Source dialog box, fill in the source **Node**, card **Slot**, **Port**, and **Type** where the test set is connected and click the **Next** button.
- **f.** In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the DS-N port in the destination node) and click the **Finish** button.

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

Note Loopbacks operate only on ports in the OOS_MT state.

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

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

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

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

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

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

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

f. Click the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit on the Destination XTC Port" procedure on page 1-13.

Procedure: Test the Terminal Loopback Circuit on the Destination XTC Port

Step 1 If the test set is not already sending traffic, send test-set 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:

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

b. Clear the terminal loopback circuit:
  - Click the **Circuits** tab.
  - Choose the loopback circuit being tested.
  - Click the **Delete** button.
  - Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "Perform a Hairpin on a Destination Node XTC Port" procedure on page 1-14.

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

Step 5 Proceed to the "Test the Destination XTC Card" procedure on page 1-14.

Procedure: Test the Destination XTC Card

Step 1 Replace the suspect card with a good card. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective XTC card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:

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

d. Clear the terminal loopback circuit:

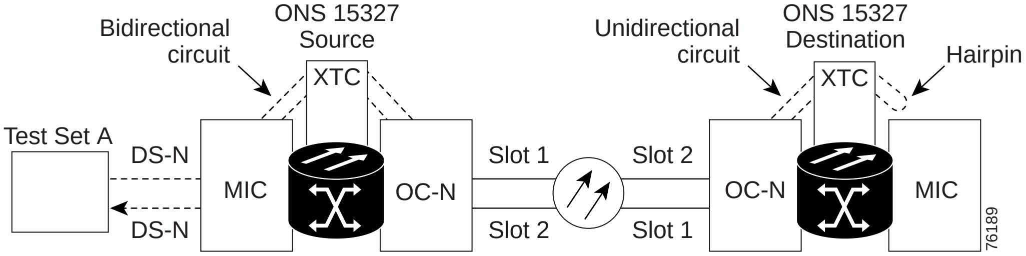
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.2.4 Perform a Hairpin on a Destination Node XTC Port" section on page 1-14.

1.2.4 Perform a Hairpin on a Destination Node XTC Port

The hairpin test is preformed on the XTC card in the destination node. To perform this test, you must also create a bidirectional circuit from the source MIC card to the source OC-N node in the transmit direction. Creating the bidirectional circuit and completing a successful hairpin isolates the possibility that the source and destination OC-N cards, the source and destination XTC cards, or the fiber span is responsible for the faulty circuit. Figure 1-10 on page 1-15 shows an example of a hairpin circuit on a destination node XTC card.

Figure 1-10 Hairpin on a Destination Node XTC Card



Procedure: Create the Hairpin Loopback Circuit on the Destination Node XTC Card

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

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

Step 2 Use CTC to set up the source loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the port in the destination node) and click the **Finish** button.

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

Step 4 Use CTC to set up the destination hairpin circuit on the port being tested.

Note The destination loopback circuit on a port is a one-way test.

For example, in a typical east-to-west slot configuration, a Slot 1 (east) OC-N card on the source node is one end of the fiber span, and the Slot 2 (west) OC-N card on the destination node is the other end.

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the Circuit **Type** and **Size** to the normal preferences.

d. Uncheck the **Bidirectional** check box and click the **Next** button.

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

f. In the Circuit Destination dialog box, use the same **Node**, card **Slot**, **Port**, and **Type** used for the Circuit Source dialog box and click the **Finish** button.

Step 5 Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit.

Step 6 Verify that the circuits connect to the correct slots. For example, verify that source node/Slot 1 OC-N card (east slot) is connected to destination node/Slot 2(west slot). If two east slots or two west slots are connected, the circuit does not work. Except for the distinct slots, all other circuit information, such as ports, should be identical.

Step 7 Proceed to the "Test the Hairpin Circuit" procedure on page 1-16.

Procedure: Test the Hairpin Circuit

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

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information indicated by the test set.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit:

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the hairpin circuit is deleted from the Circuits tab list.

b. Proceed to the "Perform a Facility Loopback on a Destination XTC Card" procedure on page 1-18.

Step 4 If the test set indicates a faulty circuit, the problem might exist with the destination XTC card.

Step 5 Proceed to the "Test the Alternate Destination XTC Card" procedure on page 1-16.

Procedure: Test the Alternate Destination XTC Card

Step 1 Perform a software reset on the active XTC card.

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

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

Step 2 Resend test traffic on the loopback circuit. The test traffic routes through the alternate XTC card.

Step 3 If the test set indicates a faulty circuit, assume that the XTC card is not causing the problem:

a. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.

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

b. Proceed to the "Perform a Facility Loopback on a Destination XTC Card" procedure on page 1-18.

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

Step 5 To confirm a defective original XTC card, proceed to the "Retest the Original Destination XTC Card" procedure on page 1-17.

Procedure: Retest the Original Destination XTC Card

Step 1 Perform a side switch of the XTC cards to make the original card the active card.

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

Step 2 Resend test traffic on the loopback circuit. The test traffic routes through the original XTC card.

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

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the defective cross-connect card. See "Physically Replace a Card" procedure on page 2-130.

c. Clear the hairpin circuit:

- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the XTC card might have had a temporary problem that is cleared by the side switch.

Clear the hairpin circuit:

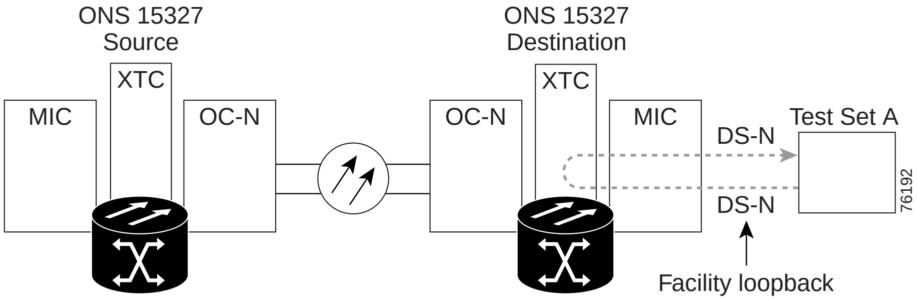
- Click the **Circuits** tab.
- Choose the hairpin circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 5 Proceed to the "1.2.5 Perform a Facility Loopback on a Destination XTC Card" section on page 1-18.

1.2.5 Perform a Facility Loopback on a Destination XTC Card

The facility loopback test is performed on the last port in the circuit, in this case the XTC port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination node cabling, MIC card, or line interface is responsible for a faulty circuit. Figure 1-11 shows an example of a facility loopback on a destination node XTC port.

Figure 1-11 Facility Loopback on a Destination XTC Card



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

Note Loopbacks operate only on ports in the OOS_MT state.

Procedure: Create a Facility Loopback Circuit on a Destination XTC Port

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

a. If you just completed the "Perform a Hairpin on a Destination Node XTC Port" procedure on page 1-14, leave the electrical test set hooked up to the DS-N port in the destination node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

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

d. Click the **Apply** button.

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

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

Step 3 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-19.

Procedure: Test the Facility Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the loopback circuit.

a. Clear the facility loopback:

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

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

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty MIC card or faulty cabling from the MIC card to the XTC card.

Step 5 Proceed to the "Test the DS-N Cabling" procedure on page 1-6.

Procedure: Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC ports) with a good cable.

If a good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable:

a. Replace the defective cable.

b. Clear the facility loopback:

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

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

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

Step 5 Proceed to the "Test the XTC Card" procedure on page 1-20.

Procedure: Test the XTC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

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

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

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

Step 5 Proceed to the "Test the MIC Card" procedure on page 1-20.

Procedure: Test the MIC Card

Step 1 Replace the suspect card with a card known to be good.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (Cisco TAC).

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

- Click the **Maintenance** > **Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.

- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

Step 4 If the test set indicates a faulty circuit, contact the Cisco TAC.

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

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

The example in this section tests an OC-N circuit on a three-node BLSR. Using a series of facility loopbacks and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of seven network test procedures applies to this sample scenario:

1. Facility loopback on the source-node OC-N port
2. Cross-connect loopback on the source-node OC-N port
3. Terminal loopback on the source-node OC-N port
4. Facility loopback on the intermediate-node OC-N port
5. Terminal loopback on the intermediate-node OC-N port
6. Facility loopback on the destination-node OC-N port
7. Terminal loopback on the destination-node OC-N port

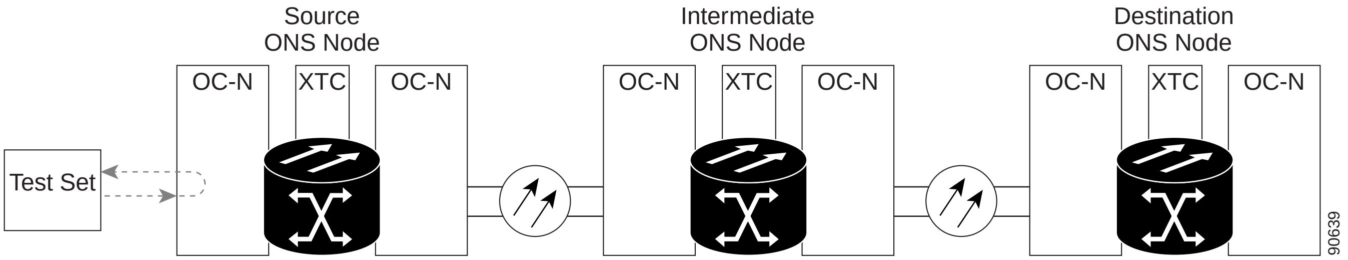
Note The test sequence for your circuits differs according to the type of circuit and network topology.

Note All loopback tests require on-site personnel.

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

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the source node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-12 on page 1-22 shows an example of a facility loopback on a circuit source OC-N port.

Figure 1-12 Facility Loopback on a Circuit Source OC-N Port



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

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

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

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

Step 2 Use CTC to create the facility loopback circuit on the port being tested:

a. In node view, double-click the card where you are performing the loopback.

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

c. Choose **OOS_MT** from the State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

d. 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.

e. Click the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

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

Step 3 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-22.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:

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

- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

b. Proceed to the "Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-23.

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-23.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

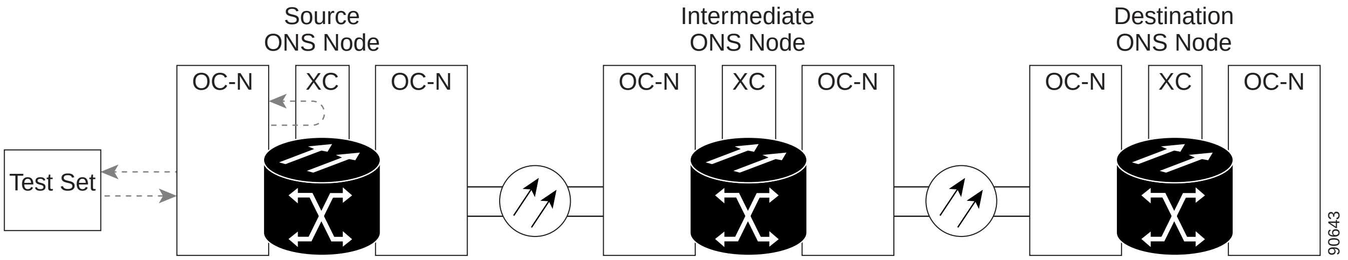
- Click the **Maintenance** > **Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation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

Step 4 Proceed to the "1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port" section on page 1-23.

1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port

The cross-connect loopback test occurs on the cross-connect card (XCT) in a network circuit. A cross-connect loopback circuit uses the same port for both source and destination. Completing a successful cross-connect loopback through the XCT card isolates the possibility that the XCT card is the cause of the faulty circuit. Figure 1-13 on page 1-24 shows an example of a cross-connect loopback on a source OC-N port.

Figure 1-13 Cross-Connect Loopback on a Source OC-N Port



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

a. If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port" section on page 1-21, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

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

a. In node view, double-click the card where the test set is connected. The card view appears.

b. In card view, click the **Provisioning** > **Line** tabs.

c. Choose **OOS** or **OOS_MT** from the Status column for the port being tested.

d. Click **Apply**.

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

Step 3 Use CTC to set up the cross-connect loopback on the circuit being tested:

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

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

c. Click **Apply**.

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

Step 4 Proceed to the "Test the Cross-Connect Loopback Circuit" procedure on page 1-24.

Procedure: Test the Cross-Connect Loopback Circuit

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

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

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

a. Clear the cross-connect loopback:

- In card view, click the **Provisioning** > **SONET STS** tabs.
- Uncheck the check box in the XC Loopback column for the circuit being tested.

- Click **Apply**.
- Click **Yes** in the confirmation dialog.

b. Proceed to the "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-27.

Step 4 If the test set indicates a faulty circuit, there might be a problem with the cross-connect card.

Step 5 Proceed to the "Test the Standby XTC Card" procedure on page 1-25.

Procedure: Test the Standby XTC Card

Step 1 Perform a reset on the active XTC card:

a. Determine which cross-connect card is active. On both the physical node and the CTC window, the active XTC has a green ACT LED, and the standby XTC has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby XTC displays a green ACT LED.
- The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
- The LEDs should complete this sequence within 5 to 10 minutes.

Step 2 Resend test traffic on the loopback circuit.

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

Step 3 If the test set indicates a faulty circuit, assume that the cross-connect card is not causing the problem:

a. Clear the cross-connect loopback circuit:

- Click the **Circuits** tab.
- Choose the cross-connect loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.
- Confirm that the cross-connect loopback circuit is deleted from the Circuits tab list.

b. Proceed to "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-27.

Step 4 If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 Proceed to the "Retest the Original XTC Card" procedure on page 1-26.

Procedure: Retest the Original XTC Card

Step 1 Do a manual switch of the XTC cards to make the original XTC card the active card:

a. Determine the active cross-connect card. On both the physical node and the CTC window, the active XTC has a green ACT LED, and the standby XTC has an amber SBY LED.

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

c. Right-click and choose **Reset** from the shortcut menu.

d. On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message is displayed.

e. Click **OK**. On the network view map, the node where you reset the XTC is gray.

f. After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby XTC displays a green ACT LED.
- The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode).
- The LEDs should complete this sequence within 5 to 10 minutes.

Step 2 Resend test traffic on the loopback circuit.

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

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty XTC card. See "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the cross-connect loopback:

- Click the **Circuits** tab.
- Choose the cross-connect loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

d. Proceed to Step 5.

Step 4 If the test set indicates a good circuit, the XTC card might have had a temporary problem that is cleared by the switch.

Clear the cross-connect loopback:

a. Click the **Circuits** tab.

b. Choose the cross-connect loopback circuit being tested.

c. Click the **Delete** button.

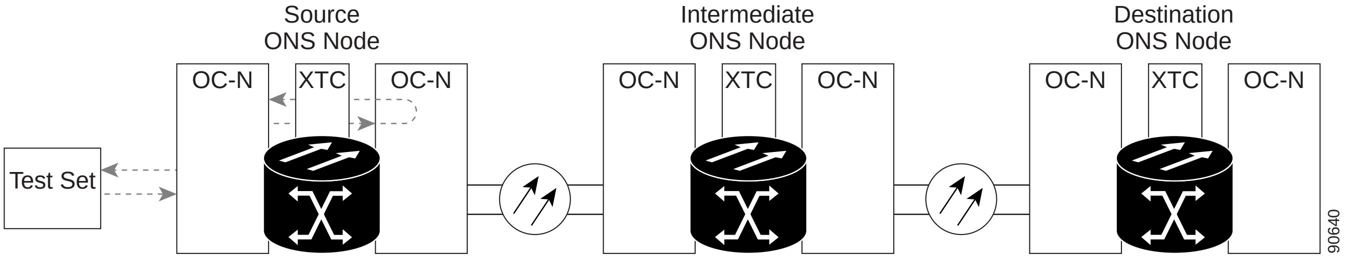
d. Click the **Yes** button in the Delete Circuits dialog box.

Step 5 Proceed to the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-27.

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

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the source node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. Figure 1-14 shows an example of a terminal loopback on a source node OC-N port.

Figure 1-14 Terminal Loopback on a Source-Node OC-N Port



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

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

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

a. If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port" section on page 1-21, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN2.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the source node) and click the **Finish** button.

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

Note It is normal for a LPBKTERMINAL condition 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. In node view, double-click the card that requires the loopback, such as the destination OC-N card in the source node.

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

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

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

e. Click the **Apply** button.

f. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-28.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:

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

b. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-29.

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-29.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

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

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

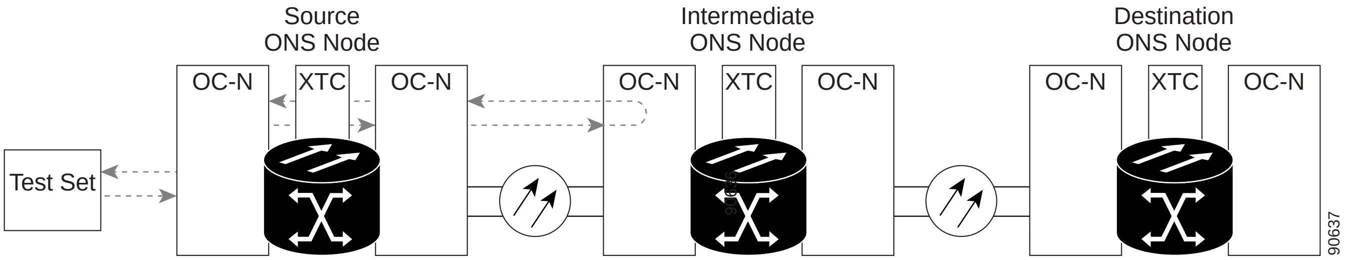
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" section on page 1-29.

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

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the intermediate node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-15 on page 1-30 shows an example of a facility loopback on a intermediate node circuit source OC-N port.

Figure 1-15 Facility Loopback on an Intermediate-Node OC-N Port



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

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

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

a. If you just completed the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-27, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN3.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.

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

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

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

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

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

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

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

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

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

f. Click the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

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

Step 5 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-31.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:

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

b. Clear the facility loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" section on page 1-32.

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-32.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

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

d. Clear the facility loopback circuit:

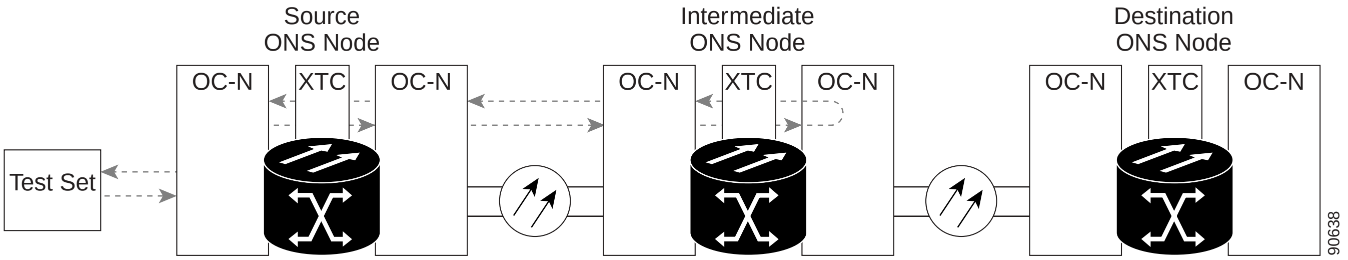
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" section on page 1-32.

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

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the intermediate node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N port. Figure 1-16 on page 1-33 shows an example of a terminal loopback on an intermediate node destination OC-N port.

Figure 1-16 Terminal Loopback on an Intermediate-Node OC-N Port



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

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

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

a. If you just completed the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" section on page 1-29, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN4.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the intermediate node) and click the **Finish** button.

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

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

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

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

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

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

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

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

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

f. Click the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-34.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:

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

b. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" section on page 1-35.

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-34.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:

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

d. Clear the terminal loopback circuit:

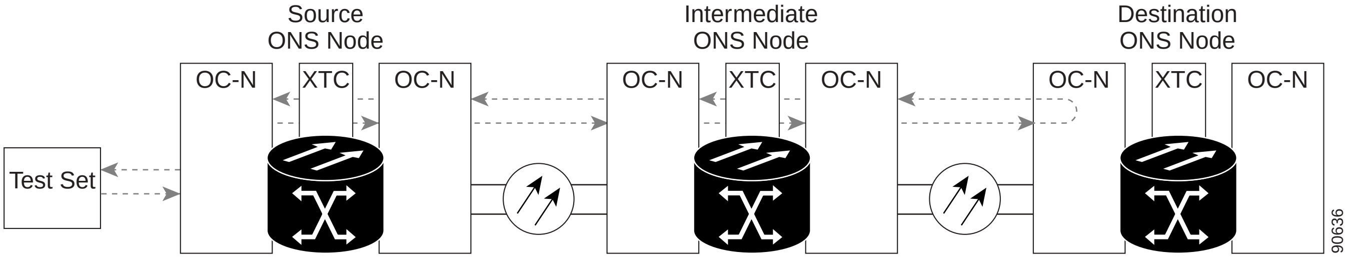
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" section on page 1-35.

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

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

Figure 1-17 Facility Loopback on a Destination Node OC-N Port



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

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

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

a. If you just completed the "Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-32, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN5.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.

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

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

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

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

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

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

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

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

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

f. Click the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

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

Step 5 Proceed to the "Test the Facility Loopback Circuit" procedure on page 1-31.

Procedure: Test the Facility Loopback Circuit

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

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

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

a. Clear the facility loopback:
   - Click the **Maintenance > Loopback** tabs.
   - Choose **None** from the Loopback Type column for the port being tested.
   - Choose the appropriate state (IS, OOS, or OOS_AINS) from the State column for the port being tested.
   - Click the **Apply** button.
   - Click the **Yes** button in the confirmation dialog box.

b. Clear the facility loopback circuit:
   - Click the **Circuits** tab.
   - Choose the loopback circuit being tested.
   - Click the **Delete** button.
   - Click the **Yes** button in the Delete Circuits dialog box.

c. Proceed to the "1.3.7 Perform a Terminal Loopback on a Destination Node OC-N Port" section on page 1-38.

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-37.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the facility loopback:

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

d. Clear the facility loopback circuit:

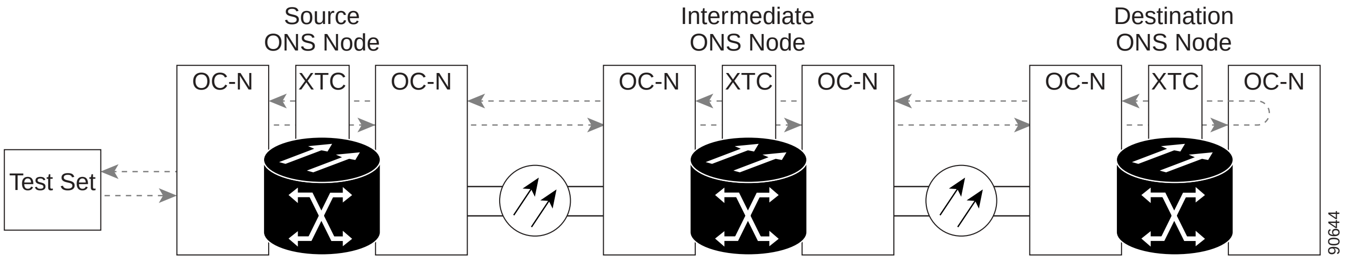
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 Proceed to the "1.3.7 Perform a Terminal Loopback on a Destination Node OC-N Port" section on page 1-38.

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

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

Figure 1-18 Terminal Loopback on a Destination Node OC-N Port



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

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

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

a. If you just completed the "Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-35, leave the optical test set hooked up to the OC-N port in the source node.

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

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click the **Create** button.

b. Give the circuit an easily identifiable name, such as OCN1toOCN6.

c. Set circuit **Type** and **Size** to the normal preferences.

d. Leave the **Bidirectional** check box checked and click the **Next** button.

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

f. In the Circuit Destination dialog box, fill in the destination **Node**, card **Slot**, **Port**, and **Type** (the OC-N port in the destination node) and click the **Finish** button.

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

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

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

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

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

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

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

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

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

f. Click the **Apply** button.

g. Click the **Yes** button in the Confirmation Dialog box.

Step 5 Proceed to the "Test the Terminal Loopback Circuit" procedure on page 1-40.

Procedure: Test the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:

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

b. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

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

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

Step 5 Proceed to the "Test the OC-N Card" procedure on page 1-40.

Procedure: Test the OC-N Card

Step 1 Replace the suspect card with a card known to be good. See the "Physically Replace a Card" procedure on page 2-130 for details.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card:

a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Contact the Cisco TAC.

b. Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-130 for details.

c. Clear the terminal loopback:

- Double-click the OC-N card in the source node with the terminal loopback.
- Click the **Maintenance** > **Loopback** tabs.
- Select **None** from the Loopback Type column for the port being tested.

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

d. Clear the terminal loopback circuit:

- Click the **Circuits** tab.
- Choose the loopback circuit being tested.
- Click the **Delete** button.
- Click the **Yes** button in the Delete Circuits dialog box.

Step 4 The entire OC-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.4 Restoring the Database and Default Settings

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

1.4.1 Restore the Node Database

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

Table 1-1 on page 1-41 describes the potential cause of the symptom and the solution.

Table 1-1 Restore the Node Database

Possible Problem	Solution
Incorrect or corrupted node database.	Perform a Restore the Database procedure. Refer to the "Restore the Database" procedure on page 1-41.

Procedure: Restore the Database

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

Caution E10/100-4 cards lose traffic for approximately 90 seconds when an ONS 15327 database is restored. Traffic is lost during the period of spanning-tree reconvergence. The CARLOSS alarm appears and clears during this period.

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

Step 1 Log into the node where you are restoring the database.

a. On the PC connected to the ONS 15327, start Netscape or Internet Explorer.

b. In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15327 IP address.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages display while CTC files are downloaded to your computer. The first time you connect to an ONS 15327, this process can take several minutes. After the download, the CTC Login dialog box displays.

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

Step 2 Ensure that there are no ring or span switch events; that is, ring-switch east or west, and span-switch east or west. In network view, click the **Conditions** tab and click **Retrieve Conditions** to view a list of conditions.

Step 3 If there are switch events that need to be cleared, in node (default) view, click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

a. If there is a switch event (not caused by a line failure), clear the switch by choosing **CLEAR** from the drop-down menu and click **Apply**.

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

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

Step 5 Click **Restore**.

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

Step 7 Click the database file to highlight it.

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

Caution Opening a restore file from another node or from an earlier backup 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 XTC card.

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

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

1.4.2 Restore the Node to Factory Configuration

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

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

Table 1-2 Restore the Node to Factory Configuration

Possible Problem	Solution
Failure of both XTC cards in the node.	To restore the node to factory configuration, see the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-43 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-45. This procedure describes how to restore the node to factory configuration using the RE-INIT.jar JAVA file, which is referred to as the reinitialization tool in this documentation. Use this tool to upload the software package and/or restore the database after it has been backed up. You need the CD containing the latest software, the node's NE defaults, and the recovery tool.
Replacement of both XTC cards at the same time.	

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

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

Note If the software package files and database backup files are located in different directories, complete the Package and Database fields (Figure 1-19 on page 1-44).

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

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

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

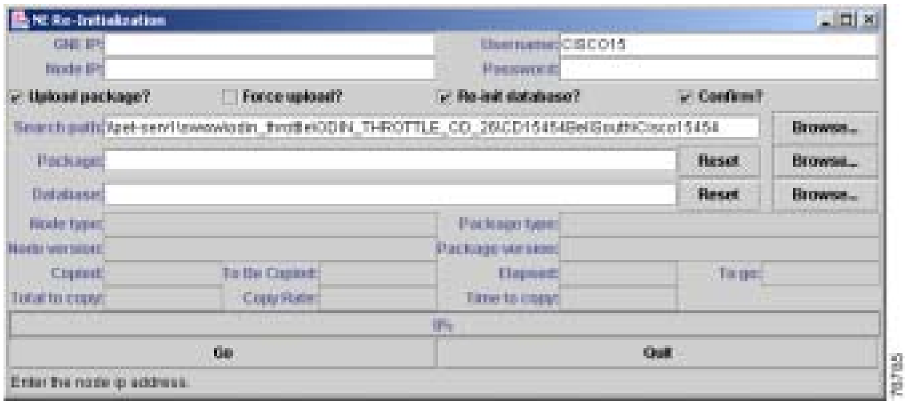
Step 1 Insert the system software CD containing the reinit tool (Figure 1-19) into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

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

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

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

Figure 1-19 Reinitialization Tool in Windows



GNE IP:
Node IP:
Username: CISCO15
Password:
☑ Upload package? □ Force upload? ☑ Re-init database? ☑ Confirm?
Search path: \\pet-serv1\swrowlasdin_throttle\ODIN_THROTTLE_CD_26\CD15454\BellSouth\Cisco15454
Package:
Database:
Enter the node ip address.

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

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

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

Step 8 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

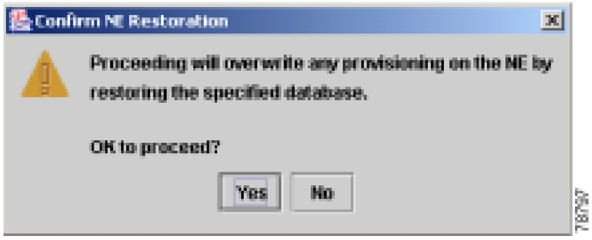
Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool chooses the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally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

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

Step 9 Click **Go**.

Step 10 A confirmation dialog box opens (Figure 1-20). Click **Yes**.

Figure 1-20 Confirm NE Restoration



Confirm NE Restoration

Proceeding will overwrite any provisioning on the NE by restoring the specified database.

OK to proceed?

Step 11 The status bar at the bottom of the window displays Complete when the node has activated the software and uploaded the database.

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

Step 12 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the XTC or on the hub or switch to which the ONS 15327 is physically connected.

Step 13 Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15327 Procedure Guide*.

Step 14 Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15327 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

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

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

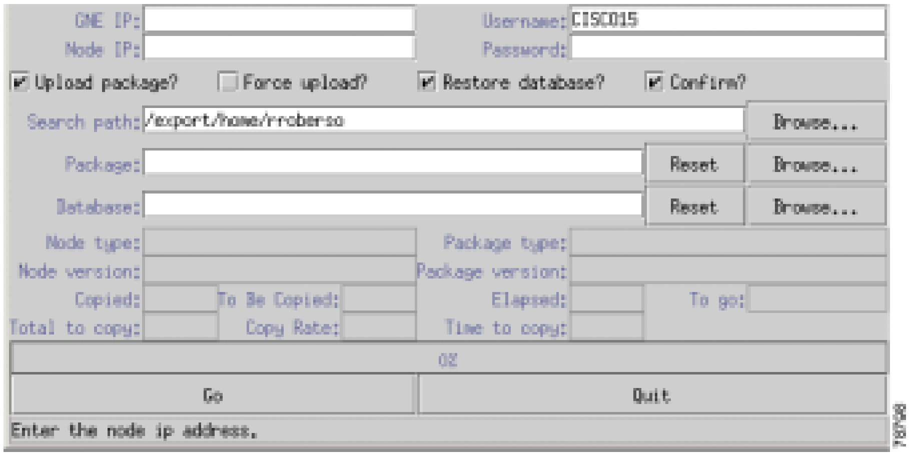
Note The XTC cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

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

Step 3 If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinit tool (Figure 1-21). If you are working with a command line interface, run **`java -jar RE-INIT.jar`**.

Figure 1-21 Reinitialization Tool in UNIX



GNE IP:
Node IP:
Username: CISCO15
Password:
☑ Upload package? ☐ Force upload? ☑ Restore database? ☑ Confirm?
Search path: /export/home/rroberso
Package:
Database:
Node type:
Node version:
Package type:
Package version:
Copied:
To Be Copied:
Elapsed:
To go:
Total to copy:
Copy Rate:
Time to copy:
0%
Enter the node ip address.

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

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-21).

Step 6 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If any are not checked, click that check box.

Step 7 In the Search Path field, verify that the path to the CISCO15454 folder on the CD drive is listed.

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinit tool 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 Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

Step 8 Click **Go**.

Step 9 A confirmation dialog box opens (Figure 1-20 on page 1-45). Click **Yes.**

Step 10 The status bar at the bottom of the window displays Complete when the node has activated the software and uploaded the database.

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

Step 11 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the XTC or on the hub or switch to which the ONS 15327 is physically connected.

Step 12 Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15327 Procedure Guide*.

Step 13 Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15327 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

1.5 PC Connectivity Troubleshooting

This section contains troubleshooting procedures for PC and network connectivity to the ONS 15327.

1.5.1 Unable to Verify the IP Configuration of Your PC

Symptom When connecting your PC to the ONS 15327, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

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

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

Possible Problem	Solution
The IP address is typed incorrectly.	Verify that the IP address used to ping the PC matches the IP address displayed when the Windows IP Configuration information is retrieved from the system.
The IP configuration of your PC is not properly set.	Verify the IP configuration of your PC, see the "Verify the IP Configuration of Your PC" procedure on page 1-47. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Procedure: Verify the IP Configuration of Your PC

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

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

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

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

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

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

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

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

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

1.5.2 Browser Login Does Not Launch Java

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

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

Table 1-4 Browser Login Does Not Launch Java

Possible Problem	Solution
The PC operating system and browser are not properly configured.	Reconfigure the PC operating system java plug-in control panel and the browser settings. See the “Reconfigure the PC Operating System Java Plug-in Control Panel” procedure on page 1-48 and the “Reconfigure the Browser” procedure on page 1-48.

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

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

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

- **a.** Run the Cisco ONS 15327 software CD.
- **b.** Open the *CD-drive*:\Windows\JRE folder.
- **c.** Double-click the **j2re-1_3_1_02-win** icon to run the JRE installation wizard.
- **d.** Follow the JRE installation wizard steps.

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

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

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

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

Step 7 Click the **Apply** button.

Step 8 Close the Java Plug-in Control Panel window.

Procedure: Reconfigure the Browser

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

Step 2 If you are using Netscape Navigator:

a. From 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 the **OK** button.

d. From 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 95/98/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 the **Choose Folder** button.

h. Navigate to the file listed in step f and click the **OK** button.

i. Click the **OK** button 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 v1.3.1_02 for <applet> (requires restart)** check box.

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

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.6.3 Browser Stalls When Downloading CTC JAR Files from XTC" section on page 1-54.

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 into the ONS 15327.

Step 7 After completing browser configuration, enable the virus-scanning software on the computer.

1.5.3 Unable to Verify the NIC Connection on Your PC

Symptom When connecting your PC to the ONS 15327, you are unable to verify that the NIC connection is working properly because the link LED is not illuminated or flashing.

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

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

Possible Problem	Solution
The Category 5 cable is not plugged in properly.	Confirm both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.
The Category 5 cable is damaged.	Ensure that the cable is in good condition. If in doubt, use a cable known to be good. Often, cabling is damaged due to pulling or bending.

Table 1-5 Unable to Verify the NIC Connection on Your PC (continued)

Possible Problem	Solution
Incorrect type of Category 5 cable is being used.	If connecting an ONS 15327 directly to your laptop/PC or a router, use a straight-through Category 5 cable. When connecting the ONS 15327 to a hub or a LAN switch, use a crossover Category 5 cable. For details on the types of Category 5 cables, see the "1.8.2.1 Crimp Replacement LAN Cables" section on page 1-74.
The NIC is improperly inserted or installed.	If you are using a PCMCIA-based NIC, remove and re-insert the NIC to make sure the NIC is fully inserted. If the NIC is built into the laptop/PC, verify that the NIC is not faulty.
The NIC is faulty.	Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.5.4 Verify PC Connection to the ONS 15327 (Ping)

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

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

Table 1-6 Verify PC Connection to ONS 15327 (Ping)

Possible Problem	Solution
A lost connection between the PC and the ONS 15327.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15327 XTC card. A ping command works if the PC connects directly to the XTC card or uses a LAN to access the XTC card. See the "Ping the ONS 15327" procedure on page 1-50.

Procedure: Ping the ONS 15327

Step 1 Display the command prompt:

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

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

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

```
ping ONS-15327-IP-address
```

For example:

```
ping 192.1.0.2.
```

Step 3 If the workstation has connectivity to the ONS 15327, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message displays.

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

Step 5 If the ping is not successful and the workstation connects to the ONS 15327 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 15327, check that the link light on the workstation's NIC is illuminated.

1.5.5 The IP Address of the Node is Unknown

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

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

Table 1-7 Retrieve the Unknown IP Address of the Node

Possible Problem	Solution
The node is not set to the default IP address.	Leave one XTC card in the shelf. Connect a PC directly to the remaining XTC card and perform a hardware reset of the XTC card. The XTC card transmits the IP address during the reset to enable you to capture the IP address for login after the XTC has completed reset. See the "Retrieve Unknown Node IP Address" procedure on page 1-51.

Procedure: Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active XTC 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 XTC card.

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

1.6 CTC Operation Troubleshooting

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

1.6.1 Unable to Launch CTC Help After Removing Netscape

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

Table 1-8 describes the potential cause of the symptom and the solution.

Table 1-8 Unable to Launch CTC Help After Removing Netscape

Possible Problem	Solution
Loss of association between browser and Help files.	When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Set Internet Explorer as the default browser so that CTC will associate the Help files to the correct browser. See the "Set Internet Explorer as the Default Browser for CTC" procedure on page 1-52 to associate the CTC Help files to the correct browser.

Procedure: Set 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 the **OK** button.

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.

1.6.2 Unable to Change Node View to Network View

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

Table 1-9 on page 1-53 describes the potential cause of the symptom and the solution.

Table 1-9 Browser Stalls When Downloading Files From XTC

Possible Problem	Solution
The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.	Reset the system or user CTC_HEAP environment variable to increase the memory limits. See the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-53 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-53 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.

Procedure: Reset the CTC_HEAP Environment Variable for Windows

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

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

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

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

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

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

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

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

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

Step 10 You can now restart the browser and CTC software.

Procedure: Reset the CTC_HEAP Environment Variable for Solaris

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

Step 2 Kill any Netscape applications.

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

```
% setenv CTC_HEAP 256
```

Step 4 You can now restart the browser and CTC software in the same user shell window.

1.6.3 Browser Stalls When Downloading CTC JAR Files from XTC

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

Table 1-10 describes the potential cause of the symptom and the solution.

Table 1-10 Browser Stalls When Downloading JAR File from XTC

Possible Problem	Solution
McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.	Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scan" procedure on page 1-54.

Procedure: Disable the VirusScan Download Scan

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

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

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

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

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

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

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

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

Step 9 Close the McAfee VirusScan window.

1.6.4 CTC Does Not Launch

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

Table 1-11 describes the potential cause of the symptom and the solution.

Table 1-11 CTC Does Not Launch

Possible Problem	Solution
The Netscape browser cache might point to an invalid directory.	Redirect the Netscape cache to a valid directory. See the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-55.

Procedure: Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 Display the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand **Advanced** and select 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.

1.6.5 Sluggish CTC Operation or Login Problems

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

Table 1-12 describes the potential cause of the symptom and the solution.

Table 1-12 Sluggish CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Delete the CTC cache file. This operation forces the ONS 15327 to download a new set of JAR files to your computer hard drive. See the "Delete the CTC Cache File Automatically" procedure on page 1-55 or the "Delete the CTC Cache File Manually" procedure on page 1-56.

Procedure: Delete the CTC Cache File Automatically

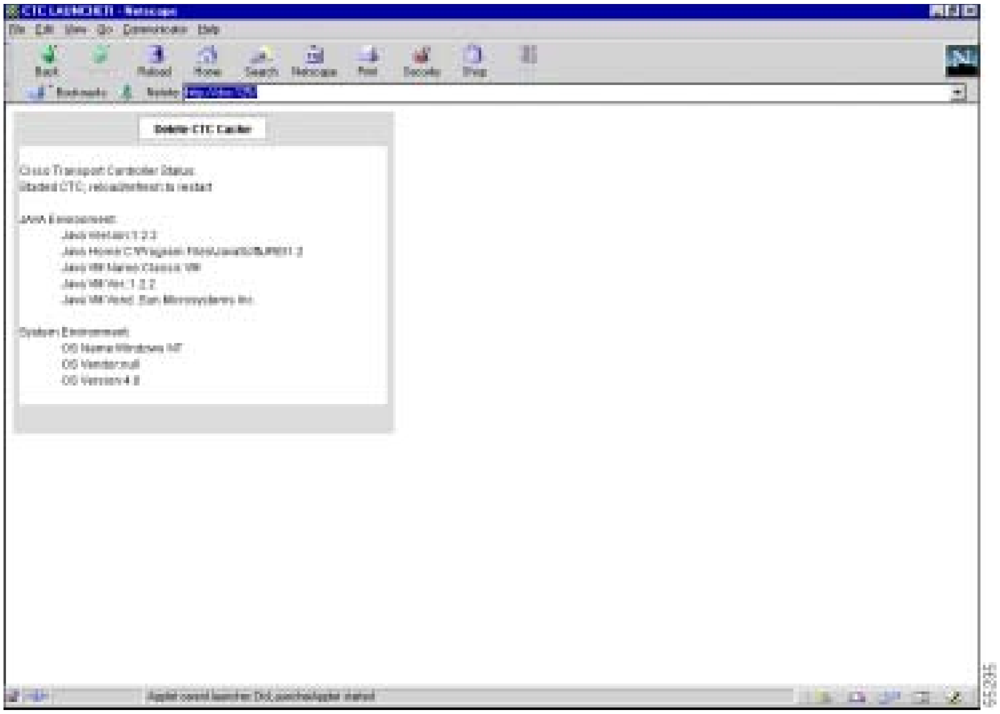
Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC sessions running on this system to behave in an unexpected manner.

Step 1 Enter an ONS 15327 IP address in 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 the **Delete CTC Cache** button on the initial browser window to clear the CTC cache. Figure 1-22 on page 1-56 shows the Delete CTC Cache window.

Figure 1-22 Deleting the CTC Cache



Cisco Transport Controller Status:
Started CTC; reload/refresh to restart

JAVA Environment:
Java Version:1.2.2
Java Home:C:\Program Files\JavaSoft\JRE\1.2
Java VM Name:Classic VM
Java VM Ver.:1.2.2
Java VM Vend.:Sun Microsystems Inc.

System Environment:
OS Name:Windows NT
OS Vendor:null
OS Version:4.0

Procedure: 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 on the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column on the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the XTC. 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.

1.6.6 Node Icon is Gray on CTC Network View

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

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

Table 1-13 Node Icon is Gray on CTC Network View

Possible Problem	Solution
Different CTC releases are not recognizing each other.	Usually accompanied by an INCOMPATIBLE-SW alarm. Correct the core version build as described in the "1.6.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-59.
A username/password mismatch.	Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the "1.6.10 Username or Password Does Not Match the XTC Information" section on page 1-60.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.6.15 Ethernet Connections" section on page 1-62.
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.49 EOC" section on page 2-48.

1.6.7 CTC Cannot Launch Due to Applet Security Restrictions

Symptom The error message "Unable to launch CTC due to applet security restrictions" appears after you enter the IP address in the browser window.

Table 1-14 describes the potential cause(s) of the symptom and the solution(s).

Table 1-14 CTC Cannot Launch Due to Applet Security Restrictions

Possible Problem	Solution
Did not execute the javapolicyinstall.bat file.	**1.** Verify that you have executed the javapolicyinstall.bat file on the ONS 15327 software CD. This file is installed when you run the CTC Setup Wizard. (Refer to the CTC installation information in the *Cisco ONS 15327 Procedure Guide* for instructions). **2.** If you ran the javapolicyinstall.bat file but still receive the error message, you must manually edit the java.policy file on your computer. See the "Manually Edit the java.policy File" procedure on page 1-58.
The java.policy file might be incomplete.	

Procedure: Manually Edit the java.policy File

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

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

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

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

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

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as ".java.policy." On Windows 95, 98, and 2000 PCs, save the file to the C:\Windows folder. On Windows NT 4.0 PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.6.8 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Table 1-15 describes the potential cause of the symptom and the solution.

Table 1-15 Java Runtime Environment Incompatible

Possible Problem	Solution
The compatible Java 2 JRE is not installed.	The Java 2 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 15327 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 15327 software CD and on the Cisco ONS 15327 documentation CD. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-59. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with all of the releases that you are running. See Table 1-16 on page 1-59.

Table 1-16 on page 1-59 shows JRE compatibility with ONS 15327 software releases.

Table 1-16 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15327 Release 1.0.0	Yes	No
ONS 15327 Release 1.0.1	Yes	Yes
ONS 15327 Release 2.2.1 and earlier	Yes	No
ONS 15327 Release 2.2.2	Yes	Yes
ONS 15327 Release 3.0	Yes	Yes
ONS 15327 Release 3.1	Yes	Yes
ONS 15327 Release 3.2	Yes	Yes
ONS 15327 Release 3.3	Yes	Yes
ONS 15327 Release 3.4	No	Yes

Procedure: Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 Type the ONS 15327 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 Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to both the ONS 15327 and ONS 15454, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a Version 2.3 core build and a Version 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.

1.6.9 Different CTC Releases Do Not Recognize Each Other

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

Table 1-17 on page 1-60 describes the potential cause of the symptom and the solution.

Table 1-17 Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the XTC card are incompatible.	This occurs when the XTC software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. **Note** Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or earlier and then attempt to log into another ONS node in the network running a later CTC core version, the earlier version node does not recognize the new node. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-60.

Procedure: Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

Step 3 In the Node Name field, type the ONS 15327 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 XTC.

1.6.10 Username or Password Does Not Match the XTC Information

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

Table 1-18 describes the potential cause(s) of the symptom and the solution(s).

Table 1-18 Username or Password Does Not Match the XTC Information

Possible Problem	Solution
The username or password entered does not match the information stored in the XTC.	All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial logon to the ONS 15327, type the CISCO15 username in capital letters and click **Login** (no password is required). If you are using CTC Software Release 2.2.2 or earlier and CISCO15 does not work, type cerent454 for the username. See the "Verify Correct Username and Password" procedure on page 1-61.

Procedure: Verify Correct Username and Password

Step 1 Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.

Step 2 Contact your system administrator to verify the username and password.

Step 3 Call Cisco TAC to have them enter your system and create a new user name and password.

1.6.11 No IP Connectivity Exists Between Nodes

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

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

Table 1-19 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
Lost Ethernet connection	Usually, this condition is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.6.15 Ethernet Connections" section on page 1-62.

1.6.12 DCC Connection Lost

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

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

Table 1-20 DCC Connection Lost

Possible Problem	Solution
A lost DCC connection	Usually, this condition is accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.49 EOC" section on page 2-48.

1.6.13 "Path in Use" Error When Creating a Circuit

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

Table 1-21 on page 1-62 describes the potential cause of the symptom and the solution.

Table 1-21 "Path in Use" Error When Creating a Circuit

Possible Problem	Solution
Another user has already selected the same source port to create another circuit	CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. See the "Cancel the Circuit Creation and Start Over" procedure on page 1-62.

Procedure: Cancel the Circuit Creation and Start Over

Step 1 Cancel the circuit creation:

- Click the **Cancel** button.
- Click the **Back** button until you return to the initial circuit creation window.

Step 2 Check the list of available ports. The previously selected port no longer appears in the available list because it is now part of a provisioned circuit.

Step 3 Select a different available port and begin the circuit creation process.

1.6.14 Calculate and Design IP Subnets

Symptom You cannot calculate or design IP subnets on the ONS 15327.

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

Table 1-22 Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15327 require specific calculations to properly design IP subnets.	Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15327 IP capability, refer to the *Cisco ONS 15327 Reference Manual*.

1.6.15 Ethernet Connections

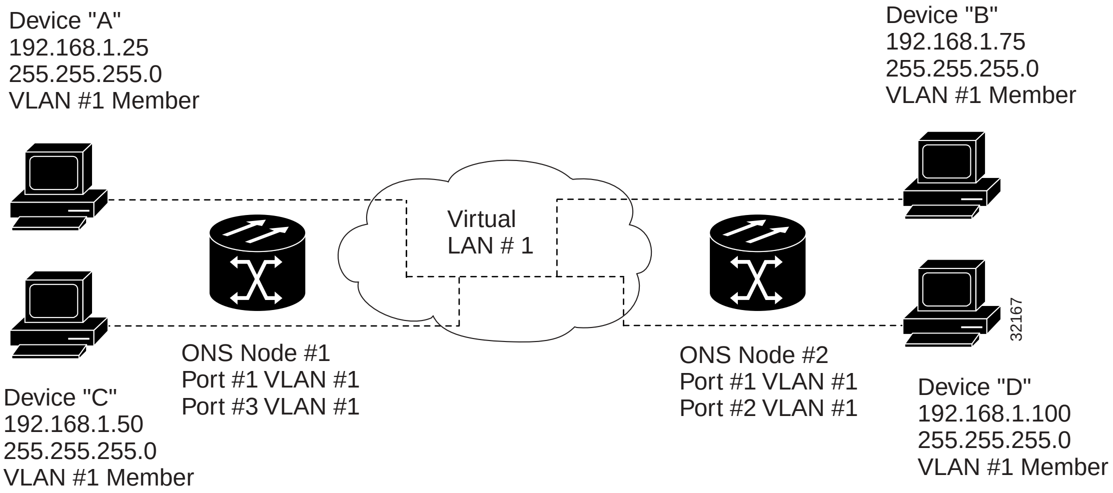
Symptom Ethernet connections appear to be broken or are not working properly.

Table 1-23 on page 1-63 describes the potential cause(s) of the symptom and the solution(s).

Table 1-23 Ethernet Connections

Possible Problem	Solution
Improperly seated connections	You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-23 when consulting the steps in the "Verify Ethernet Connections" procedure on page 1-63.
Incorrect connections	

Figure 1-23 Ethernet Connectivity Reference



Procedure: Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET alarms on the STS-N that carries the VLAN #1 Ethernet circuit. Clear any alarms by looking them up in Chapter 2, "Alarm Troubleshooting."

Step 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 15327 #1 and Ports 1 and 2 on ONS 15327 #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 15327s 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 an Ethernet cable known to be good.

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

e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Run the procedure in the "1.9.3 Lamp Test for Card LEDs" section on page 1-80.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices (see the "1.5.4 Verify PC Connection to the ONS 15327 (Ping)" section on page 1-50). If the ping is unsuccessful:

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

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

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

Step 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 15327 #1 and ONS 15327 #2 ports also use VLAN #1.

1.6.16 VLAN Cannot Connect to Network Device from Untag Port

Symptom Networks that have a VLAN with one ONS 15327 Ethernet card port set to Tagged and one ONS 15327 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-24). They might also see a higher than normal runt packets count at the network device attached to the Untag port.This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Figure 1-24 VLAN with Ethernet Ports at Tagged and Untag

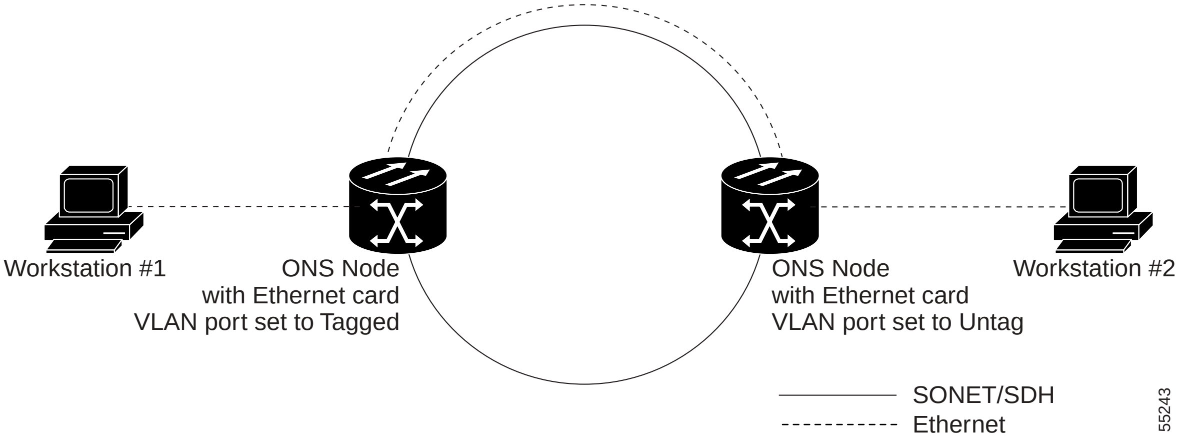


Table 1-24 on page 1-65 describes the potential cause(s) of the symptom and the solution(s).

Table 1-24 VLAN Cannot Connection to Network Device from Untag Port

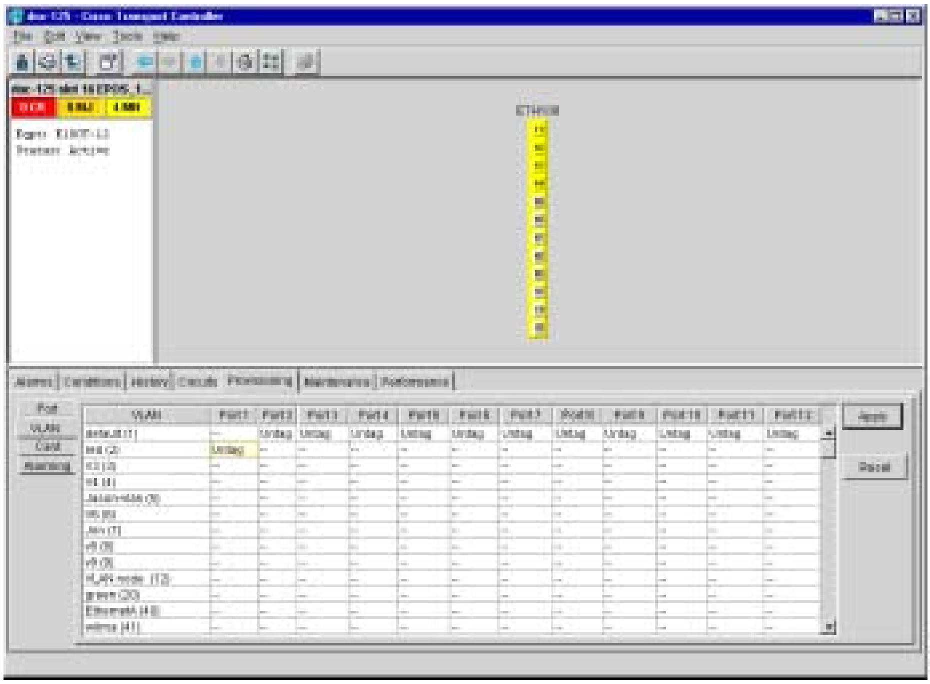
Possible Problem	Solution
The Tagged ONS 15327 adds the IEEE 802.1Q tag and the Untag ONS 15327 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.	See the "Change VLAN Port Tag and Untagged Settings" procedure on page 1-65. The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevents the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards can 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 lose IEEE 802.1Q compliance.
Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.	

Procedure: Change VLAN Port Tag and Untagged Settings

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

Step 2 Click the **Provisioning** > **VLAN** tabs (Figure 1-25).

Figure 1-25 Configuring VLAN Membership for Individual Ethernet Ports



VLAN	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10	Port11	Port12
default (1)	--	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag
[illegible] (2)	Untag	--	--	--	--	--	--	--	--	--	--	--
[illegible] (3)	--	--	--	--	--	--	--	--	--	--	--	--
[illegible] (4)	--	--	--	--	--	--	--	--	--	--	--	--
[illegible] (5)	--	--	--	--	--	--	--	--	--	--	--	--
[illegible] (6)	--	--	--	--	--	--	--	--	--	--	--	--
[illegible] (7)	--	--	--	--	--	--	--	--	--	--	--	--
v8 (8)	--	--	--	--	--	--	--	--	--	--	--	--
v9 (9)	--	--	--	--	--	--	--	--	--	--	--	--
VLAN node (12)	--	--	--	--	--	--	--	--	--	--	--	--
green (20)	--	--	--	--	--	--	--	--	--	--	--	--
EthernetA (40)	--	--	--	--	--	--	--	--	--	--	--	--
[illegible] (41)	--	--	--	--	--	--	--	--	--	--	--	--

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

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

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

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

1.7 Circuits and Timing

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

1.7.1 Circuit Transitions to Partial State

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

- OOS_PARTIAL—At least one of the connections in the circuit is in OOS state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.
- OOS_MT_PARTIAL—At least one connection in the circuit is in OOS_MT state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.
- OOS_AINS_PARTIAL—At least one connection in the circuit is in the OOS_AINS state and at least one other connection in the circuit is in IS or OOS_AINS state.

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

Table 1-25 Circuit in Partial State

Possible Problem	Solution
During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.	Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-67. Log onto 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 15327 Software Upgrade Guide* for software upgrade procedures. **Note** If the node software cannot be upgraded to Software R3.4, the partial state condition can be avoided by only using the circuit state(s) supported in the earlier software release.

Table 1-25 Circuit in Partial State (continued)

Possible Problem	Solution
During an automatic transition, some path-level defects and/or alarms were detected on the circuit.	Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-67. Log into 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 15327 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.
One end of the circuit is not properly terminated.	

Procedure: View the State of Circuit Nodes

Step 1 Click the **Circuits** tab.

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

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

Step 4 In the Edit Circuit window, click the **State** tab.

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

1.7.2 AIS-V on XTC-28-3 Unused VT Circuits

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

Table 1-26 describes the potential cause of the symptom and the solution.

Table 1-26 AIS-V on XTC-28-3 Unused VT Circuits

Possible Problem	Solution
The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.	An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on XTC-28-3 VT circuits that are not carrying traffic and on stranded bandwidth. Perform the "Clear AIS-V on XTC-28-3 Unused VT Circuits" procedure on page 1-67.

Procedure: Clear AIS-V on XTC-28-3 Unused VT Circuits

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, and 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 XTC-28-3 card in CTC card view. Click the **Maintenance** > **DS1** tabs.

Step 7 Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

Step 8 From the Loopback Type list, choose **Facility (line)** and click **Apply**.

Step 9 Click **Circuits**.

Step 10 Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**.

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

Step 12 Display the XTC-28-3 card in CTC card view. Click **Maintenance** > **DS1**.

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

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

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

Step 16 Repeat this procedure for all the AIS-V alarms on the XTC-28-3 cards.

1.7.3 Circuit Creation Error with VT1.5 Circuit

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

Table 1-27 describes the potential cause(s) of the symptom and the solution(s).

Table 1-27 Circuit Creation Error with VT1.5 Circuit

Possible Problem	Solution
You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15327 indicated in the error message.	The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a UPSR or 1+1 protection group. Refer to the *Cisco ONS 15327 Reference Manual* for more information.

1.7.4 DS3 Card Does Not Report AIS-P From External Equipment

Symptom A DS-3 card does not report STS AIS-P from the external equipment/line side.

Table 1-28 describes the potential cause of the symptom and the solution.

Table 1-28 DS3 Card Does Not Report AIS-P From External Equipment

Possible Problem	Solution
The card is functioning as designed.	This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. DS-3 cards have DS-3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS-3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information on the PM capabilities of the DS-3 cards, refer to the *Cisco ONS 15327 Procedure Guide*.

1.7.5 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Table 1-29 describes the potential cause of the symptom and the solution.

Table 1-29 OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the ONS 15327.	For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15327 Procedure Guide*.

1.7.6 ONS 15327 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

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

Table 1-30 ONS 15327 Switches Timing Reference

Possible Problem	Solution
The optical or building integrated timing supply (BITS) input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.	The ONS 15327 internal clock operates at a Stratum 3 level of accuracy. This gives the ONS 15327 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} per day, including temperature. ONS 15327 free-running synchronization relies on the Stratum 3 internal clock. Use a higher quality Stratum 1 or Stratum 2 timing source. This results in fewer timing slips than a lower quality Stratum 3 timing source.
The optical or BITS input is not functioning.	
Synchronization status message (SSM) is set to Don't Use for Synchronization (DUS).	
SSM indicates a Stratum 3 or lower clock quality.	
The input frequency is off by more than 15 ppm.	
The input clock wanders and has more than three slips in 30 seconds.	
A bad timing reference existed for at least two minutes.	

1.7.7 Holdover Synchronization Alarm

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

Table 1-31 describes the potential cause of the symptom and the solution.

Table 1-31 Holdover Synchronization Alarm

Possible Problem	Solution
The last reference input has failed.	The clock is running at the frequency of the last valid reference input. This alarm is raised when the last reference input fails. See the "2.6.94 HLDOVRSYNC" section on page 2-73 for a detailed description of this alarm. **Note** The ONS 15327 supports holdover timing per Telcordia GR-4436 when provisioned for external (BITS) timing.

1.7.8 Free-Running Synchronization Mode

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

Table 1-32 describes the potential cause of the symptom and the solution.

Table 1-32 Free-Running Synchronization Mode

Possible Problem	Solution
No reliable reference input is available.	The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "2.6.90 FRNGSYNC" section on page 2-71 for a detailed description of this alarm.

1.7.9 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy-chain the BITS.

Table 1-33 describes the potential cause of the symptom and the solution.

Table 1-33 Daisy-Chained BITS Not Functioning

Possible Problem	Solution
Daisy-chaining BITS is not supported on the ONS 15327.	Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15327.

1.7.10 Blinking STAT LED after Installing a Card

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

Table 1-34 describes the potential cause of the symptom and the solution.

Table 1-34 Blinking STAT LED on Installed Card

Possible Problem	Solution
The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.	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-BOOT alarm is raised against the slot number with an "Equipment Fails To Boot" description. Check the alarm tab for this alarm to appear for the slot where the card is installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card.

1.8 Fiber and Cabling

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

1.8.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Table 1-35 describes the potential cause of the symptom and the solution.

Table 1-35 Bit Errors Appear for a Line Card

Possible Problem	Solution
Faulty cabling or low optical-line levels.	Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Moving cards into different error-free slots isolates 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 15327. Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using the "1.8.2 Faulty Fiber-Optic Connections" section on page 1-72.

1.8.2 Faulty Fiber-Optic Connections

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

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

Table 1-36 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections.	Faulty fiber-optic connections can be the source of SONET alarms and signal errors. See the "Verify Fiber-Optic Connections" procedure on page 1-72.
Faulty Category-5 cables.	Faulty Category-5 cables can be the source of SONET alarms and signal errors. See the "1.8.2.1 Crimp Replacement LAN Cables" section on page 1-74.
Faulty gigabit interface connectors.	Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the "1.8.2.2 Replace Faulty SFP Connectors" section on page 1-76.

Warning **Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector.**

Warning **Class IIIb laser.**

Warning **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.**

Warning **Avoid direct exposure to the beam. Invisible radiation is emitted from the aperture at the end of the fiber optic cable when connected, but not terminated.**

Procedure: Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15327 card.

SM or SM Fiber should be printed on the fiber span cable. ONS 15327 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 that the power meter is set to the appropriate wavelength for the optical card being tested (either 1310 nm or 1550 nm depending on the specific card).

e. Verify that the power level falls within the range specified for the card; see the "1.8.2.3 Optical Card Transmit and Receive Levels" section on page 1-77.

Step 4 If the power level falls below the specified range:

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 15327 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

b. Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15327 Procedure Guide*. If possible, do this for the 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 card to eliminate the possibility of a degrading transmitter on this card.

e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

- Excessive fiber distance—Single-mode fiber attenuates at approximately 0.5 dB/km.
- Excessive number or fiber connectors—Connectors take approximately 0.5 dB each.
- Excessive number of fiber splices—Splices take approximately 0.5 dB each.

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

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the optical card failed:

a. Check that the 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 15327 Procedure Guide*. If possible, do this for the card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the optical card.

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

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

Receiver overloads occur when maximum receiver power is exceeded.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the card transmitter and the receiver. Place the attenuator on the receive transmitter of the 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.

1.8.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15327. Use a cross-over cable when connecting an ONS 15327 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15327 to a router or workstation. Use #22 or #24 AWG shielded wire with RJ-45 connectors, and a crimping tool. Figure 1-26 shows the layout of an RJ-45 connector.

Figure 1-26 RJ-45 Pin Numbers

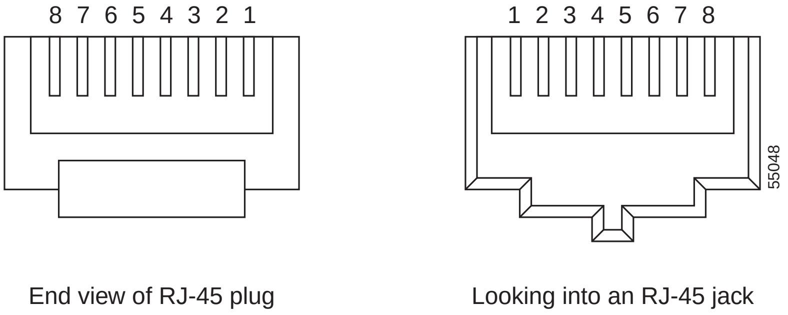


Figure 1-27 shows the layout of a LAN cable.

Figure 1-27 LAN Cable Layout

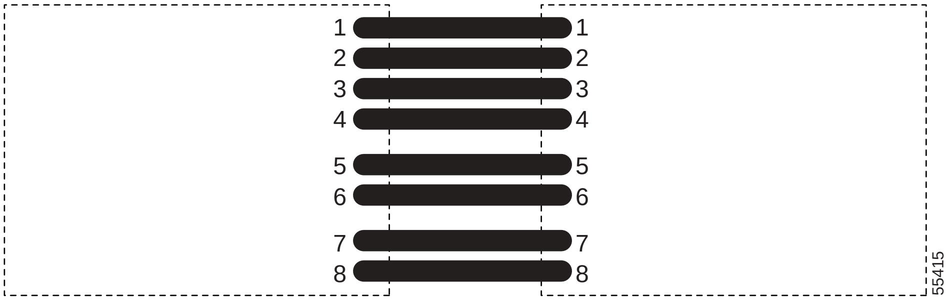


Table 1-37 shows the pinout of a LAN cable.

Table 1-37 LAN Cable Pinout

Pin	Color	Pair	Name	Pin
1	White/orange	2	Transmit Data +	1
2	Orange	2	Transmit Data -	2
3	White/green	3	Receive Data +	3
4	Blue	1		4
5	White/blue	1		5
6	Green	3	Receive Data -	6
7	White/brown	4		7
8	Brown	4		8

Figure 1-28 on page 1-75 shows the layout of a cross-over cable.

Figure 1-28 Cross-Over Cable Layout

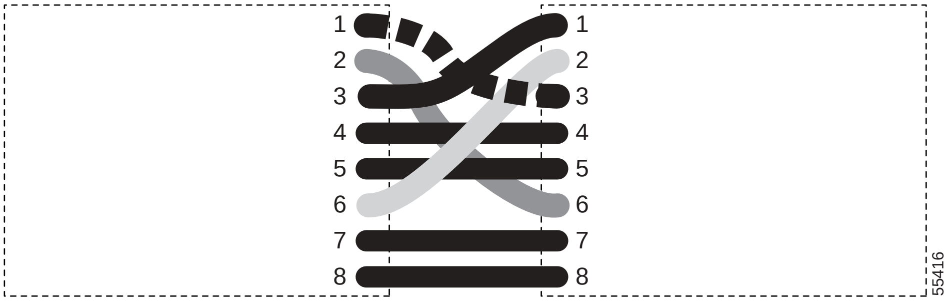


Table 1-38 shows the pinout of a cross-over cable.

Table 1-38 Cross-Over Cable Pinout

Pin	Color	Pair	Name	Pin
1	White/orange	2	Transmit Data +	3
2	Orange	2	Transmit Data –	6
3	White/green	3	Receive Data +	1
4	Blue	1		4
5	White/blue	1		5
6	Green	3	Receive Data –	2
7	White/brown	4		7
8	Brown	4		8

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

1.8.2.2 Replace Faulty SFP Connectors

Small Form-factor Pluggable (SFP) connectors are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

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

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

SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of SFPs and their capabilities, see Table 1-39 on page 1-76 and refer to the *Cisco ONS 15327 Reference Manual*.

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

Table 1-39 Available SFP Connectors

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	G1000-2	Short reach	Multimode fiber up to 550 m long	15327-SFP-LC-SX=
1000BaseLX	G1000-2	Long reach	Single-mode fiber up to 5 km long	15327-SFP-LC-LX=

Procedure: Remove SFP Connectors

Step 1 Disconnect the network fiber cable from the SFP LC duplex connector.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Step 2 Release the SFP from the slot by simultaneously squeezing the two plastic tabs on each side.

Step 3 Slide the SFP out of the Gigabit Ethernet module slot. A flap closes over the SFP slot to protect the connector on the Gigabit Ethernet card.

Procedure: Install SFP Connectors

Step 1 Remove the SFP from its protective packaging.

Step 2 Check the label to verify that the SFP is the correct type (SX or LX) for your network.

Step 3 Verify that you are installing compatible SFPs; for example, SX to SX, LX to LX.

Step 4 Grip the sides of the SFP with your thumb and forefinger and insert the SFP into the slot on the G1000-2 card.

Note SFPs are keyed to prevent incorrect installation.

Step 5 Slide the SFP through the flap that covers the opening until you hear a click. The click indicates the SFP is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the SFP and save the plug for future use.

1.8.2.3 Optical Card Transmit and Receive Levels

Each G1000-2 and OC-N card has a transmit and receive connector on its faceplate. Table 1-40 describes the SFPs and their capabilities.

Table 1-40 Optical Card Transmit and Receive Levels

Optical Card	Receive	Transmit
G1000-2	–8 to –28 dBm	–8 to –15 dBm
OC3 IR 4 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 IR 1310	–8 to –28 dBm	–8 to –15 dBm
OC12 LR 1550	–8 to –28 dBm	+2 to –3 dBm
OC48 IR 1310	0 to –18 dBm	0 to –5 dBm
OC48 LR 1550	–8 to –28 dBm	+3 to –2 dBm

1.9 Power and LED Tests

This section provides symptoms and solutions for power supply problems, power consumption, and LED indicators.

1.9.1 Power Supply Problems

Symptom Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

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

Table 1-41 Power Supply Problems

Possible Problem	Solution
Loss of power or low voltage	The ONS 15327 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 15327 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15327 or can affect several pieces of equipment on the site. **Note** A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15327 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning** > **General** tabs and change the Date and Time fields. See the "Isolate the Cause of Power Supply Problems" procedure on page 1-79.
Improperly connected power supply	

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 15327. 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 15327 are service-affecting.

Procedure: Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15327 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 15327 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 brown-outs 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.

1.9.2 Power Consumption for Node and Cards

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

Table 1-42 describes the potential cause of the symptom and the solution.

Table 1-42 Power Consumption for Node and Cards

Possible Problem	Solution
Improper power supply.	Refer to power information in the *Cisco ONS 15327 Procedure Guide*.

1.9.3 Lamp Test for Card LEDs

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

Table 1-43 describes the potential cause of the symptom and the solution.

Table 1-43 Lamp Test for Card LEDs

Possible Problem	Solution
Faulty LED	A lamp test verifies that all the card LEDs work. Run this diagnostic test as part of the initial ONS 15327 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. See the "Verify Card LED Operation" procedure on page 1-80.

Procedure: Verify Card LED Operation

Step 1 Click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the LEDs on the cards illuminate for several seconds.

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

If an LED does not light up, the LED is faulty. Call the Cisco TAC and fill out an RMA to return the card.

CHAPTER 2

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for commonly encountered Cisco ONS 15327 alarms and conditions. Table 2-1 on page 2-1 through Table 2-4 on page 2-3 give lists of ONS 15327 alarms organized by severity. Table 2-5 on page 2-4 gives a list of alarm organized alphabetically. Table 2-6 on page 2-6 gives a list of alarms organized by alarm type. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

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

For alarm profile information, refer to the *Cisco ONS 15327 Procedure Guide*.

2.1 Alarm Index by Default Severity

The alarm index by severity tables group alarms and conditions by the severity displayed in the CTC Alarms window in the severity (SEV) column. The default standby severity for all ONS 15327 alarms on unprovisioned card ports is Minor, Non-Service Affecting, as defined in Telcordia GR-474. All severities listed in the alarm entry are the default for the active card, if applicable. Alarm severities can be altered from default settings for individual alarms or groups of alarms on a card, node, or network basis.

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

2.1.1 Critical Alarms (CR)

Table 2-1 lists Critical alarms.

Table 2-1 Critical Alarm Index

BKUPMEMP, page 2-29	HITEMP, page 2-72	MEA (EQPT), page 2-90
COMIOXC, page 2-37	IMPROPRMVL, page 2-73	MFGMEM, page 2-92
CTNEQPT-PBPROT, page 2-41	LOF (DS-3), page 2-79	PLM-P, page 2-95
CTNEQPT-PBWORK, page 2-43	LOF (OC-N), page 2-80	SWMTXMOD, page 2-113

Table 2-1 Critical Alarm Index (continued)

EQPT, page 2-50	LOP-P, page 2-80	TIM-P, page 2-119
EQPT-MISS, page 2-51	LOS (DS-3), page 2-83	UNEQ-P, page 2-122
FAN, page 2-59	LOS (OC-N), page 2-84	

2.1.2 Major Alarms (MJ)

Table 2-2 lists Major alarms.

Table 2-2 Major Alarm Index

APSCM, page 2-21	EOC, page 2-48	MEM-GONE, page 2-91
APSCNMIS, page 2-21	E-W-MISMATCH, page 2-51	PEER-NORESPONSE, page 2-94
BLSROSYNC, page 2-30	EXTRA-TRAF-PREEMPT, page 2-54	PRC-DUPID, page 2-96
CARLOSS (EQPT), page 2-31	FANDEGRADE, page 2-60	RCVR-MISS, page 2-100
CARLOSS (E Series), page 2-32	INVMACADR, page 2-76	RING-MISMATCH, page 2-103
CARLOSS (G Series), page 2-33	LOF (BITS), page 2-77	SYSBOOT, page 2-119
CONTBUS-A-18, page 2-37	LOF (DS-1), page 2-78	TPTFAIL (G-Series), page 2-120
CONTBUS-B-18, page 2-38	LOP-V, page 2-81	TRMT, page 2-120
CONTBUS-IO-A, page 2-38	LOS (BITS), page 2-81	TRMT-MISS, page 2-121
CONTBUS-IO-B, page 2-40	LOS (DS-1), page 2-82	UNEQ-V, page 2-123
DBOSYNC, page 2-45		

2.1.3 Minor Alarms (MN)

Table 2-3 lists Minor alarms.

Table 2-3 Minor Alarm Index

APSB, page 2-18	ELWBATVG-A, page 2-47	PWR-A, page 2-98
APSCDFLTK, page 2-18	ELWBATVG-B, page 2-47	PWR-B, page 2-99
APSC-IMP, page 2-19	EXCCOL, page 2-53	PWR-REDUN, page 2-100
APSCINCON, page 2-20	EXT, page 2-54	SFTWDOWN, page 2-107
APSMM, page 2-22	FEPRLF, page 2-69	SNTP-HOST, page 2-108
AUTORESET, page 2-25	FSTSYNC, page 2-71	SSM-FAIL, page 2-110
AUTOSW-LOP (VTMON), page 2-26	HITEMP, page 2-72	SYNCPRI, page 2-117
AUTOSW-UNEQ (VTMON), page 2-28	MEM-LOW, page 2-92	SYNCSEC, page 2-117
DATAFLT, page 2-44	PLM-V, page 2-96	SYNCTHIRD, page 2-118
EHIBATVG-A, page 2-46	PROTNA, page 2-97	TIM-P, page 2-119
EHIBATVG-B, page 2-46		

2.1.4 Conditions (NA or NR)

Table 2-4 lists Not Alarmed or Not Reported conditions.

Table 2-4 Conditions Index

AIS, page 2-16	FE-FRCDWKSWPR-SPAN, page 2-65	MANUAL-REQ-SPAN, page 2-90
AIS-L, page 2-16	FE-IDLE, page 2-66	PDI-P, page 2-93
AIS-P, page 2-17	FE-LOCKOUTOFPR-SPAN, page 2-66	RAI, page 2-100
AIS-V, page 2-17	FE-LOF, page 2-67	RFI-L, page 2-101
AS-CMD, page 2-23	FE-LOS, page 2-67	RFI-P, page 2-102
AS-MT, page 2-23	FE-MANWKSWPR-RING, page 2-68	RFI-V, page 2-102
AUD-LOG-LOSS, page 2-24	FE-MANWKSWPR-SPAN, page 2-68	RING-SW-EAST, page 2-104
AUD-LOG-LOW, page 2-24	FORCED-REQ, page 2-69	RING-SW-WEST, page 2-104
AUTOSW-AIS, page 2-25	FORCED-REQ-RING, page 2-69	SD, page 2-104
AUTOSW-LOP (STSMON), page 2-26	FORCED-REQ-SPAN, page 2-70	SD-L, page 2-105
AUTOSW-PDI, page 2-26	FRCDSWTOINT, page 2-70	SD-P, page 2-105
AUTOSW-SDBER, page 2-27	FRCDSWTOPRI, page 2-70	SF, page 2-106
AUTOSW-SFBER, page 2-27	FRCDSWTOSEC, page 2-71	SF-L, page 2-106
AUTOSW-UNEQ (STSMON), page 2-27	FRCDSWTOTHIRD, page 2-71	SF-P, page 2-107
BAT-A-HGH-VLT, page 2-28	FRNGSYNC, page 2-71	SPAN-SW-EAST, page 2-108
BAT-A-LOW-VLT, page 2-28	FULLPASSTHR-BI, page 2-72	SPAN-SW-WEST, page 2-108
BAT-B-HGH-VLT, page 2-29	HLDOVRSYNC, page 2-73	SQUELCH, page 2-109
BAT-B-LOW-VLT, page 2-29	INC-ISD, page 2-75	SSM-DUS, page 2-110
CLDRESTART, page 2-36	INHSWPR, page 2-75	SSM-LNC, page 2-111
DS3-MISM, page 2-45	INHSWWKG, page 2-75	SSM-OFF, page 2-111
EXERCISE-RING-REQ, page 2-53	KB-PASSTHR, page 2-76	SSM-PRC, page 2-111
EXERCISE-SPAN-REQ, page 2-53	LKOUTPR-S, page 2-76	SSM-PRS, page 2-111
FAILTOSW, page 2-54	LOCKOUT-REQ, page 2-77	SSM-RES, page 2-112
FAILTOSW-PATH, page 2-55	LOCKOUT-REQ-RING, page 2-77	SSM-SMC, page 2-112
FAILTOSWR, page 2-56	LPBKCRS, page 2-86	SSM-ST2, page 2-112
FAILTOSWS, page 2-58	LPBKFACILITY (DS-N), page 2-86	SSM-ST3, page 2-112
FE-AIS, page 2-60	LPBKFACILITY (OC-N), page 2-87	SSM-ST3E, page 2-112
FE-DS1-MULTLOS, page 2-61	LPBKTERMINAL (DS-N, OC-N), page 2-87	SSM-ST4, page 2-113
FE-DS1-NSA, page 2-61	LPBKTERMINAL (G-Series), page 2-88	SSM-STU, page 2-113
FE-DS1-SA, page 2-62	MAN-REQ, page 2-88	SSM-TNC, page 2-113
FE-DS1-SNGLLOS, page 2-62	MANRESET, page 2-88	SWTOPRI, page 2-115
FE-DS3-NSA, page 2-63	MANSWTOINT, page 2-89	SWTOSEC, page 2-115
FE-DS3-SA, page 2-63	MANSWTOPRI, page 2-89	SWTOTHIRD, page 2-115

Table 2-4 Conditions Index (continued)

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-5 lists alarms and conditions by the name displayed on the CTC Alarms window or Conditions window.

Table 2-5 Alphabetical Alarm Index

Table 2-5 Alphabetical Alarm Index (continued)

BAT-A-HGH-VLT, page 2-28	FRCDSWTOSEC, page 2-71	SF, page 2-106
BAT-A-LOW-VLT, page 2-28	FRCDSWTOTHIRD, page 2-71	SF-L, page 2-106
BAT-B-HGH-VLT, page 2-29	FRNGSYNC, page 2-71	SF-P, page 2-107
BAT-B-LOW-VLT, page 2-29	FSTSYNC, page 2-71	SFTWDOWN, page 2-107
BKUPMEMP, page 2-29	FULLPASSTHR-BI, page 2-72	SNTP-HOST, page 2-108
BLSROSYNC, page 2-30	HITEMP, page 2-72	SPAN-SW-EAST, page 2-108
CARLOSS (EQPT), page 2-31	HLDOVRSYNC, page 2-73	SPAN-SW-WEST, page 2-108
CARLOSS (E Series), page 2-32	IMPROPRMVL, page 2-73	SQUELCH, page 2-109
CARLOSS (G Series), page 2-33	INC-ISD, page 2-75	SSM-DUS, page 2-110
CLDRESTART, page 2-36	INHSWPR, page 2-75	SSM-FAIL, page 2-110
COMIOXC, page 2-37	INHSWWKG, page 2-75	SSM-LNC, page 2-111
CONTBUS-A-18, page 2-37	INVMACADR, page 2-76	SSM-OFF, page 2-111
CONTBUS-B-18, page 2-38	KB-PASSTHR, page 2-76	SSM-PRC, page 2-111
CONTBUS-IO-A, page 2-38	LKOUTPR-S, page 2-76	SSM-PRS, page 2-111
CONTBUS-IO-B, page 2-40	LOCKOUT-REQ, page 2-77	SSM-RES, page 2-112
CTNEQPT-PBPROT, page 2-41	LOCKOUT-REQ-RING, page 2-77	SSM-SMC, page 2-112
CTNEQPT-PBWORK, page 2-43	LOF (BITS), page 2-77	SSM-ST2, page 2-112
DATAFLT, page 2-44	LOF (DS-1), page 2-78	SSM-ST3, page 2-112
DBOSYNC, page 2-45	LOF (DS-3), page 2-79	SSM-ST3E, page 2-112
DS3-MISM, page 2-45	LOF (OC-N), page 2-80	SSM-ST4, page 2-113
EHIBATVG-A, page 2-46	LOP-P, page 2-80	SSM-STU, page 2-113
EHIBATVG-B, page 2-46	LOP-V, page 2-81	SSM-TNC, page 2-113
ELWBATVG-A, page 2-47	LOS (BITS), page 2-81	SWMTXMOD, page 2-113
ELWBATVG-B, page 2-47	LOS (DS-1), page 2-82	SWTOPRI, page 2-115
EOC, page 2-48	LOS (DS-3), page 2-83	SWTOSEC, page 2-115
EQPT, page 2-50	LOS (OC-N), page 2-84	SWTOTHIRD, page 2-115
EQPT-MISS, page 2-51	LPBKCRS, page 2-86	SYNC-FREQ, page 2-116
E-W-MISMATCH, page 2-51	LPBKFACILITY (DS-N), page 2-86	SYNCPRI, page 2-117
EXCCOL, page 2-53	LPBKFACILITY (OC-N), page 2-87	SYNCSEC, page 2-117
EXERCISE-RING-REQ, page 2-53	LPBKTERMINAL (DS-N, OC-N), page 2-87	SYNCTHIRD, page 2-118
EXERCISE-SPAN-REQ, page 2-53	LPBKTERMINAL (G-Series), page 2-88	SYSBOOT, page 2-119
EXT, page 2-54	MAN-REQ, page 2-88	TIM-P, page 2-119
EXTRA-TRAF-PREEMPT, page 2-54	MANRESET, page 2-88	TPTFAIL (G-Series), page 2-120
FAILTOSW, page 2-54	MANSWTOINT, page 2-89	TRMT, page 2-120
FAILTOSW-PATH, page 2-55	MANSWTOPRI, page 2-89	TRMT-MISS, page 2-121
FAILTOSWR, page 2-56	MANSWTOSEC, page 2-89	UNEQ-P, page 2-122

Table 2-5 Alphabetical Alarm Index (continued)

FAILTOSWS, page 2-58	MANSWTOTHIRD, page 2-89	UNEQ-V, page 2-123
FAN, page 2-59	MANUAL-REQ-RING, page 2-89	WKSWPR, page 2-124
FANDEGRADE, page 2-60	MANUAL-REQ-SPAN, page 2-90	WTR, page 2-124

2.3 Alarm Index by Alarm Type

Table 2-6 gives the name and page number of every alarm in the chapter organized by alarm type.

Table 2-6 Alarm Index by Alarm Type

BITS:: LOS (BITS), page 2-81
BITS:: AIS, page 2-16
BITS:: LOF (BITS), page 2-77
BITS:: SSM-DUS, page 2-110
BITS:: SSM-FAIL, page 2-110
BITS:: SSM-OFF, page 2-111
BITS:: SSM-PRS, page 2-111
BITS:: SSM-RES, page 2-112
BITS:: SSM-SMC, page 2-112
BITS:: SSM-ST2, page 2-112
BITS:: SSM-ST3, page 2-112
BITS:: SSM-ST3E, page 2-112
BITS:: SSM-ST4, page 2-113
BITS:: SSM-STU, page 2-113
BITS:: SSM-TNC, page 2-113
DS1:: AIS, page 2-16
DS1:: AS-CMD, page 2-23
DS1:: AS-MT, page 2-23
DS1:: LOF (DS-1), page 2-78
DS1:: LOS (DS-1), page 2-82
DS1:: LPBKFACILITY (DS-N), page 2-86
DS1:: LPBKTERMINAL (DS-N, OC-N), page 2-87
DS1:: RAI, page 2-100
DS1:: RCVR-MISS, page 2-100
DS3:: SD, page 2-104
DS3:: SF, page 2-106
DS1:: TRMT, page 2-120
DS1:: TRMT-MISS, page 2-121

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

DS3:: AIS, page 2-16
DS3:: AS-CMD, page 2-23
DS3:: AS-MT, page 2-23
DS3:: DS3-MISM, page 2-45
DS3:: FE-AIS, page 2-60
DS3:: FE-DS1-MULTLOS, page 2-61
DS3:: FE-DS1-NSA, page 2-61
DS3:: FE-DS1-SA, page 2-62
DS3:: FE-DS1-SNGLLOS, page 2-62
DS3:: FE-DS3-NSA, page 2-63
DS3:: FE-DS3-SA, page 2-63
DS3:: FE-EQPT-NSA, page 2-64
DS3:: FE-IDLE, page 2-66
DS3:: FE-LOF, page 2-67
DS3:: FE-LOS, page 2-67
DS3:: INC-ISD, page 2-75
DS3:: LOF (DS-3), page 2-79
DS3:: LOS (DS-3), page 2-83
DS3:: LPBKFACILITY (DS-N), page 2-86
DS3:: LPBKTERMINAL (DS-N, OC-N), page 2-87
DS3:: RAI, page 2-100
ENV:: EXT, page 2-54
EQPT:: AS-CMD, page 2-23
EQPT:: AUTORESET, page 2-25
EQPT:: BKUPMEMP, page 2-29
EQPT:: CARLOSS (EQPT), page 2-31
EQPT:: CLDRESTART, page 2-36
EQPT:: COMIOXC, page 2-37
EQPT:: CONTBUS-A-18, page 2-37
EQPT:: CONTBUS-B-18, page 2-38
EQPT:: CONTBUS-IO-A, page 2-38
EQPT:: CONTBUS-IO-B, page 2-40
EQPT:: CTNEQPT-PBPROT, page 2-41
EQPT:: CTNEQPT-PBWORK, page 2-43
EQPT:: EQPT, page 2-50
EQPT:: EXCCOL, page 2-53
EQPT:: FAILTOSW, page 2-54

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

EQPT:: FORCED-REQ, page 2-69
EQPT:: HITEMP, page 2-72
EQPT:: IMPROPRMVL, page 2-73
EQPT:: INHSWPR, page 2-75
EQPT:: INHSWWKG, page 2-75
EQPT:: LOCKOUT-REQ, page 2-77
EQPT:: MAN-REQ, page 2-88
EQPT:: MANRESET, page 2-88
EQPT:: MEA (EQPT), page 2-90
EQPT:: MEM-GONE, page 2-91
EQPT:: MEM-LOW, page 2-92
EQPT::PEER-NORESPONSE, page 2-94
EQPT:: PROTNA, page 2-97
EQPT:: PWR-REDUN, page 2-100
EQPT:: SD, page 2-104
EQPT:: SFTWDOWN, page 2-107
EQPT:: SWMTXMOD, page 2-113
EQPT:: WKSWPR, page 2-124
EQPT:: WTR, page 2-124
ETHER:: AS-CMD, page 2-23
ETHER:: CARLOSS (E Series), page 2-32
ETHER:: CARLOSS (G Series), page 2-33
EXTSYNCH:: FRCDSWTOPRI, page 2-70
EXTSYNCH:: FRCDSWTOSEC, page 2-71
EXTSYNCH:: FRCDSWTOTHIRD, page 2-71
EXTSYNCH:: MANSWTOPRI, page 2-89
EXTSYNCH:: MANSWTOSEC, page 2-89
EXTSYNCH:: MANSWTOTHIRD, page 2-89
EXTSYNCH:: SWTOPRI, page 2-115
EXTSYNCH:: SWTOSEC, page 2-115
EXTSYNCH:: SWTOTHIRD, page 2-115
EXTSYNCH:: SYNCPRI, page 2-117
EXTSYNCH:: SYNCSEC, page 2-117
EXTSYNCH:: SYNCTHIRD, page 2-118
FAN:: EQPT-MISS, page 2-51
FAN:: FAN, page 2-59
FAN:: FANDEGRADE, page 2-60

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

FAN:: MEM-GONE, page 2-91
FAN:: MFGMEM, page 2-92
HDGE [G1000]:: AS-CMD, page 2-23
HDGE [G1000]:: AS-MT, page 2-23
HDGE [G1000]:: CARLOSS (G Series), page 2-33
HDGE [G1000]:: LPBKTERMINAL (G-Series), page 2-88
HDGE [G1000]:: TPTFAIL (G-Series), page 2-120
NBR:: SD, page 2-104
NE:: AS-CMD, page 2-23
NE:: AUD-LOG-LOW, page 2-24
NE:: AUD-LOG-LOSS, page 2-24
NE:: BAT-A-HGH-VLT, page 2-28
NE:: BAT-A-LOW-VLT, page 2-28
NE:: BAT-B-HGH-VLT, page 2-29
NE:: BAT-B-LOW-VLT, page 2-29
NE:: DATAFLT, page 2-44
NE:: DBOSYNC, page 2-45
NE:: EHIBATVG-A, page 2-46
NE:: EHIBATVG-B, page 2-46
NE:: ELWBATVG-A, page 2-47
NE:: ELWBATVG-B, page 2-47
NE:: HITEMP, page 2-72
NE:: PRC-DUPID, page 2-96
NE:: PWR-A, page 2-98
NE:: PWR-B, page 2-99
NE:: SNTP-HOST, page 2-108
NE:: SYSBOOT, page 2-119
NERING:: BLSROSYNC, page 2-30
NERING:: FULLPASSTHR-BI, page 2-72
NERING:: KB-PASSTHR, page 2-76
NERING:: PRC-DUPID, page 2-96
NERING:: RING-MISMATCH, page 2-103
NESYNCH:: FRCDSWTOINT, page 2-70
NESYNCH:: FRCDSWTOPRI, page 2-70
NESYNCH:: FRCDSWTOSEC, page 2-71
NESYNCH:: FRCDSWTOTHIRD, page 2-71
NESYNCH:: FRNGSYNC, page 2-71

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

NESYNCH:: FSTSYNC, page 2-71
NESYNCH:: HLDOVRSYNC, page 2-73
NESYNCH:: MANSWTOINT, page 2-89
NESYNCH:: MANSWTOPRI, page 2-89
NESYNCH:: MANSWTOSEC, page 2-89
NESYNCH:: MANSWTOTHIRD, page 2-89
NESYNCH:: SSM-PRS, page 2-111
NESYNCH:: SSM-RES, page 2-112
NESYNCH:: SSM-SMC, page 2-112
NESYNCH:: SSM-ST2, page 2-112
NESYNCH:: SSM-ST3, page 2-112
NESYNCH:: SSM-ST3E, page 2-112
NESYNCH:: SSM-ST4, page 2-113
NESYNCH:: SSM-STU, page 2-113
NESYNCH:: SSM-TNC, page 2-113
NESYNCH:: SWTOPRI, page 2-115
NESYNCH:: SWTOSEC, page 2-115
NESYNCH:: SWTOTHIRD, page 2-115
NESYNCH:: SYNCPRI, page 2-117
NESYNCH:: SYNCSEC, page 2-117
NESYNCH:: SYNCTHIRD, page 2-118
OCN:: AIS-L, page 2-16
OCN:: APSB, page 2-18
OCN:: APSCDFLTK, page 2-18
OCN:: APSC-IMP, page 2-19
OCN:: APSCINCON, page 2-20
OCN:: APSCM, page 2-21
OCN:: APSCNMIS, page 2-21
OCN:: APSMM, page 2-22
OCN:: AS-CMD, page 2-23
OCN:: AS-MT, page 2-23
OCN:: EOC, page 2-48
OCN:: E-W-MISMATCH, page 2-51
OCN:: EXERCISE-RING-REQ, page 2-53
OCN:: EXERCISE-SPAN-REQ, page 2-53
OCN:: EXTRA-TRAF-PREEMPT, page 2-54
OCN:: FAILTOSW, page 2-54

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

OCN:: FAILTOSWR, page 2-56
OCN:: FAILTOSWS, page 2-58
OCN:: FE-EXERCISING-RING, page 2-64
OCN:: FE-EXERCISING-SPAN, page 2-64
OCN:: FE-FRCDWKSWPR-RING, page 2-65
OCN:: FE-FRCDWKSWPR-SPAN, page 2-65
OCN:: FE-LOCKOUTOFPR-SPAN, page 2-66
OCN:: FE-MANWKSWPR-RING, page 2-68
OCN:: FE-MANWKSWPR-SPAN, page 2-68
OCN:: FEPRLF, page 2-69
OCN:: FORCED-REQ-RING, page 2-69
OCN:: FORCED-REQ-SPAN, page 2-70
OCN:: LKOUTPR-S, page 2-76
OCN:: LOCKOUT-REQ, page 2-77
OCN:: LOCKOUT-REQ-RING, page 2-77
OCN:: LOF (OC-N), page 2-80
OCN:: LOS (OC-N), page 2-84
OCN:: LPBKFACILITY (OC-N), page 2-87
OCN:: LPBKTERMINAL (DS-N, OC-N), page 2-87
OCN:: MANUAL-REQ-RING, page 2-89
OCN:: MANUAL-REQ-SPAN, page 2-90
OCN:: RFI-L, page 2-101
OCN:: RING-SW-EAST, page 2-104
OCN:: RING-SW-WEST, page 2-104
OCN:: SD-L, page 2-105
OCN:: SF-L, page 2-106
OCN:: SPAN-SW-EAST, page 2-108
OCN:: SPAN-SW-WEST, page 2-108
OCN:: SQUELCH, page 2-109
OCN:: SSM-DUS, page 2-110
OCN:: SSM-FAIL, page 2-110
OCN:: SSM-OFF, page 2-111
OCN:: SSM-PRS, page 2-111
OCN:: SSM-RES, page 2-112
OCN:: SSM-SMC, page 2-112
OCN:: SSM-ST2, page 2-112
OCN:: SSM-ST3, page 2-112

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

OCN:: SSM-ST3E, page 2-112
OCN:: SSM-ST4, page 2-113
OCN:: SSM-STU, page 2-113
OCN:: SSM-TNC, page 2-113
OCN:: SYNC-FREQ, page 2-116
OCN:: WKSWPR, page 2-124
OCN:: WTR, page 2-124
STSMON:: AIS-P, page 2-17
STSMON:: AUTOSW-AIS, page 2-25
STSMON:: AUTOSW-LOP (STSMON), page 2-26
STSMON:: AUTOSW-PDI, page 2-26
STSMON:: AUTOSW-SDBER, page 2-27
STSMON:: AUTOSW-SFBER, page 2-27
STSMON:: AUTOSW-UNEQ (STSMON), page 2-27
STSMON:: FAILTOSW-PATH, page 2-55
STSMON:: FORCED-REQ, page 2-69
STSMON:: LOCKOUT-REQ, page 2-77
STSMON:: LOP-P, page 2-80
STSMON:: LPBKCRS, page 2-86
STSMON:: MAN-REQ, page 2-88
STSMON:: PDI-P, page 2-93
STSMON:: PLM-P, page 2-95
STSMON:: RFI-P, page 2-102
STSMON:: SD-P, page 2-105
STSMON:: SF-P, page 2-107
STSMON:: TIM-P, page 2-119
STSMON:: UNEQ-P, page 2-122
STSMON:: WKSWPR, page 2-124
STSMON:: WTR, page 2-124
STSTERM:: AIS-P, page 2-17
STSTERM:: LOP-P, page 2-80
STSTERM:: PDI-P, page 2-93
STSTERM:: PLM-P, page 2-95
STSTERM:: RFI-P, page 2-102
STSTERM:: SD-P, page 2-105
STSTERM:: SF-P, page 2-107
STSTERM:: TIM-P, page 2-119

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

STSTERM:: UNEQ-P, page 2-122
VT-MON:: AIS-V, page 2-17
VT-MON:: AUTOSW-AIS, page 2-25
VT-MON:: AUTOSW-LOP (VTMON), page 2-26
VT-MON:: AUTOSW-UNEQ (VTMON), page 2-28
VT-MON:: FAILTOSW-PATH, page 2-55
VT-MON:: FORCED-REQ, page 2-69
VT-MON:: LOCKOUT-REQ, page 2-77
VT-MON:: LOP-V, page 2-81
VT-MON:: MAN-REQ, page 2-88
VT-MON:: UNEQ-V, page 2-123
VT-MON:: WKSWPR, page 2-124
VT-MON:: WTR, page 2-124
VT-TERM:: AIS-V, page 2-17
VT-TERM:: PLM-V, page 2-96
VT-TERM:: RFI-V, page 2-102
VT-TERM:: SD-P, page 2-105
VT-TERM:: SF-P, page 2-107
VT-TERM:: UNEQ-V, page 2-123

2.3.1 Alarm Type/Object Definition

Table 2-7 defines abbreviations used in the alarm troubleshooting procedures.

Table 2-7 Alarm Type/Object Definition

BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)
DS1	A DS-1 line on an XTC-14 or XTC-28-3 card
DS3	A DS-3 line on an XTC-28-3 card
ENV	An environmental alarm port on an XTC card
EQPT	A card in any of the 8 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
ETHER	Ethernet, such as for straight-through (Category 5) LAN cables
EXTSYNCH	BITS outgoing references (SYNC-BITS1, SYNC-BITS2)
FAN	Fan-tray assembly
FUDC	SONET F1 byte user data channel
HDGE	High Density Gigabit Ethernet; applies to G1000-2 cards.
MSUDC	SONET Multiplex Section User Data Channel
NE	The entire network element

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

NERING	Represents the ring status in the NE
NE-SYNCH	Represents the timing status of the NE
OCN	An OC-N line on an OCN card
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect)
STSTERM	STS alarm detection at termination (downstream from the cross-connect)
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 Trouble Notifications

The ONS 15327 uses standard Telcordia categories to characterize levels of trouble. The ONS 15327 reports alarmed trouble notifications in the CTC Alarms window and Not Alarmed (NA) trouble notifications in the Conditions window. Alarms signify a problem that the user needs to fix, such as an LOS (OC-N) alarm (see page 2-84). Conditions notify the user of an event which does not require action, such as a SWTOSEC condition (see page 2-115) or a MANRESET condition (see page 2-88).

Telcordia further divides alarms into Service-Affecting (SA) and NSA status. An SA failure affects a provided service or the network's ability to provide service. For example, a TRMT-MISS alarm (see page 2-121) is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a DS-1 port on an XTC card is removed. This affects a provided service because traffic switches to the protect card. The HITEMP alarm (see page 2-72) means that the alarm object is hotter than 122 degrees Fahrenheit (50 degrees Celsius). HITEMP is an NSA failure for a single piece of equipment, or an SA failure for the NE. For example, if the HITEMP alarm is raised against a port with an EQPT object, the alarm is NSA because port and card traffic is protected. If the HITEMP alarm is raised against the NE (shelf), however, it is an SA alarm because a high temperature affects the network's ability to provide service.

2.4.1 Conditions

When an SA failure is detected, the ONS 15327 also sends an AIS condition (see page 2-16) downstream. When the node receives the AIS, the node sends an RFI-L condition (see page 2-101) upstream. AIS and RFI belong in the conditions category and show in the Conditions window of CTC. However, unlike most conditions which are Not Alarmed (NA), Telcordia classifies these conditions as Not Reported (NR).

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

2.4.2 Severities

The ONS 15327 uses Telcordia standard severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service-affecting alarm that needs immediate correction. Major is a serious alarm, but the failure has less of an impact on the network. For example, with an LOS (DS-1), a Major alarm, 24 DS-0 circuits lose protection. But with a LOS (OC-N) for an OC-48 card, a Critical alarm, approximately 25,000 DS-0 circuits lose protection.

Minor alarms, such as the FSTSYNC alarm (see page 2-71), do not have a serious affect on service. FSTSYNC lets you know that the ONS 15327 is choosing a new timing reference because the old reference failed. The loss of the prior timing source is something a user needs to look at, but it should not immediately disrupt service.

Telcordia standard severities are the default settings for the ONS 15327. A user may customize ONS 15327 alarm severities with the alarm profiles feature. For alarm profile procedures, refer to the *Cisco ONS 15327 Procedure Guide*.

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

2.5 Safety Summary

This section covers safety considerations designed to ensure safe operation of the ONS 15327. 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 and warnings:

Caution Hazardous voltage or energy might be present when the system is operating. Use caution when removing or installing cards.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Warning **Class 1 laser product.**

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

2.6 Alarm Procedures

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

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower-right corner is not indented. If it is, click it to turn it off. When you are done checking for alarms, click the alarm filter icon again to turn filtering back on.

Note When checking alarms, make sure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, see the *Cisco ONS 15327 Procedure Guide*.

2.6.1 AIS

- Not Reported (NR), Non-Service Affecting (NSA)

The Alarm Indication Signal (AIS) condition in the SONET overhead is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service (IS) but the DS-3 or OC-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service or has an out-of-service (OOS) port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

Procedure: Clear the AIS Condition

Step 1 Verify whether there are alarms on the upstream nodes and equipment, especially an LOS (OC-N) alarm (see page 2-84) or OOS ports.

Step 2 Clear the upstream alarms using the applicable procedure(s) in this chapter.

Step 3 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.2 AIS-L

- Not Reported (NR), Non-Service Affecting (NSA)

The AIS Line (AIS-L) condition means there is an error in the SONET overhead at the line layer. The AIS-L condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS-L, for example, when the port on the reporting node is in service (IS) but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS (OC-N) alarm (see page 2-84) or has an OOS port. The AIS-L clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

Procedure: Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.3 AIS-P

- Not Reported (NR), Non-Service Affecting (NSA)

The AIS Path (AIS-P) condition means there is an error in the SONET overhead at the path layer. The AIS-P condition is secondary to another alarm occurring simultaneously in an upstream node. The AIS-P is caused by an incomplete circuit path, for example, when the port on the reporting node is in service (IS), but a node upstream on the circuit does not have its port in service. The upstream node often reports an LOS (OC-N) alarm (see page 2-84) or has an OC-N port OOS. The AIS-P clears when the primary alarm on the upstream node is cleared. However, the node with the primary alarm might not report any alarms to indicate it is at fault. AIS-P occurs at each node on the incoming OC-N path.

Procedure: Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.4 AIS-V

- Not Reported (NR), Non-Service Affecting (NSA)

The AIS Virtual Tributary (VT) condition means there is an error in the SONET overhead at the VT layer. The AIS-V condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS-V, for example, when the port on the reporting node is in service (IS) but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS (OC-N) alarm (see page 2-84) or has an OOS port. The AIS-V clears when the primary alarm is cleared. The node with the OOS port might not report any alarms to indicate it is at fault.

An AIS-V error message on the electrical card is accompanied by an AIS-P condition (see page 2-17) on the cross connected OC-N card.

Note If the AIS-V occurred on an XTC-28-3 unused circuit, complete the "Clear AIS-V on XTC-28-3 Unused VT Circuits" procedure on page 1-67.

Procedure: Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.5 APSB

- Minor (MN), Non-Service Affecting (NSA)

The Automatic Protection Switching (APS) Channel Byte Failure (APSB) alarm occurs when line terminating equipment detects protection switching byte failure in the incoming APS signal. The failure occurs when an inconsistent APS byte or invalid code is detected. Some older, non-Cisco, SONET nodes send invalid APS codes if they are configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15327. These invalid codes causes an APSB on an ONS node.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the APSB Alarm

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

For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15327.

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.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.6 APSCDFLTK

- Minor (MN), Non-Service Affecting (NSA)

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

Troubleshooting for APSCDFLTK is often similar to troubleshooting for a BLSROSYNC alarm (see page 2-30).

⚠ **Warning** **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

⚠ **Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-125 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 Node ID Number" procedure on page 2-126 to change one node's ID number so that each node ID is unique.

Step 4 If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the "E-W-MISMATCH" section on page 2-51.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15327 Procedure Guide* provides a procedure for fibering BLSRs.

Step 5 If the alarm does not clear and if the network is a BLSR, make sure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protection fiber.

Step 6 If the alarm does not clear, complete the "Verify Node Visibility for Other Nodes" procedure on page 2-126.

Step 7 If nodes are not visible, complete the "Verify or Create Node DCC Terminations" procedure on page 2-126 to ensure that SONET DCC terminations exist on each node.

Step 8 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.7 APSC-IMP

- Minor (MN), Non-Service Affecting (NSA)

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

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the APSC-IMP Alarm

Step 1 Use an optical test set to determine the validity of the K byte signal by examining the received signal.

For specific procedures to use the test set equipment, consult the manufacturer.

If the K byte is invalid, the problem is with upstream equipment and not in the reporting ONS 15327. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15327s, consult the appropriate user documentation.

Step 2 If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs. Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-125.

Step 3 Repeat Step 2 for all nodes in the ring.

Step 4 If a node has a ring ID number that does not match the other nodes, make the ring ID number of that node identical to the other nodes. Complete the "Change a Ring ID Number" procedure on page 2-125.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.8 APSCINCON

- Minor (MN), Non-Service Affecting (NSA)

An APS Inconsistent (APSCINCON) alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15327, to switch the SONET signal from a working to a protect path. An inconsistent APS code occurs when three consecutive frames do not contain identical APS bytes. Inconsistent APS bytes give the receiving equipment conflicting commands about switching.

Procedure: Clear the APSCINCON Alarm

Step 1 Look for other alarms, especially an LOS (OC-N) alarm (see page 2-84), an LOF (OC-N) alarm (see page 2-80), or an AIS condition (see page 2-16). Clearing these alarms clears the APSCINCON alarm.

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

2.6.9 APSCM

- Major (MJ), Service Affecting (SA)

The APS Channel Mismatch (APSCM) alarm occurs when the ONS 15327 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 15327 when bidirectional protection is used on OC-N cards in a 1+1 configuration.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the APSCM Alarm

Step 1 Verify that the working-card channel fibers are physically connected directly to the adjoining node’s working-card channel fibers.

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node’s protection-card channel fibers.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.10 APSCNMIS

- Major (MJ), Service Affecting (SA)

The APS Node ID Mismatch (APSCNMIS) alarm occurs when the source node ID contained in the K2 byte of the incoming APS channel is not present in the ring map. The APSCNMIS alarm might 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.

Procedure: Clear the APSCNMIS Alarm

Step 1 Complete the “Identify a Ring ID or Node ID Number” procedure on page 2-125 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 Node ID Number" procedure on page 2-126 to change one node's ID number so that each node ID is unique.

Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. The BLSR window shows the node ID of the login node.

Note Applying and removing a lock out on a span causes the ONS 15327 to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

Step 5 If the alarm does not clear, use the "Lock Out a BLSR Span" procedure on page 2-127 to lock out the span.

Step 6 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127 to clear the lock out.

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

2.6.11 APSMM

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the APSMM Alarm

Step 1 For the reporting ONS 15327, display the node view and verify the protection scheme provisioning:

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

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

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

Record whether the Bidirectional Switching check box is checked.

Step 2 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 3 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1. If not, change it to match.

Step 4 Click **Apply**.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.12 AS-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Alarms Suppressed by User Command (AS-CMD) condition applies to the network element (NE, or node) and cards. It occurs when alarms are suppressed for one or more cards or for the entire shelf.

Procedure: Clear the AS-CMD Condition

Step 1 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 window says that the object is "system," the condition applies to the shelf. Go to Step 7.

Step 3 If the AS-CMD condition is reported for a card, determine if 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 Behavior** tabs.

- If the Suppress Alarms column check box is checked for a port row, deselect the check box 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 In node view, if the AS-CMD condition is reported for a card and not an individual port, click the **Provisioning** > **Alarm Behavior** tabs.

Step 5 Locate the row for the reported card slot. (The slot number information was in the Object column in the Conditions window that you noted in Step 2.)

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 shelf, cards and other equipment are affected. To clear the alarm:

a. In node view, click the **Provisioning** > **Alarm Behavior** tabs.

b. Click the Suppress Alarms check box located at the bottom of the window to deselect the option.

c. Click **Apply**.

Step 8 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.13 AS-MT

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

Procedure: Clear the AS-MT Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.14 AUD-LOG-LOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Audit Trail Log Loss (AUD-LOG-LOS) 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.

Procedure: 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.

Note When you have archived a group of audit trail entries, they are no longer visible in CTC. The entries cannot be imported into CTC.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.15 AUD-LOG-LOW

- Not Reported (NR), Non-Service Affecting (NSA)

The Audit Trail Log Low (AUD-LOG-LOW) condition occurs when the audit trail log is 80 percent full.

Note AUD-LOG-LOW is an informational condition. It does not require troubleshooting.

2.6.16 AUTORESET

- Minor (MN), Non-Service Affecting (NSA)

The Automatic System Reset (AUTORESET) alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot. This alarm 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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the AUTORESET Alarm

Step 1 Look for any additional alarms that might have triggered an automatic reset.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Card" procedure on page 2-130.

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.17 AUTOSW-AIS

- Not Reported (NR), Non-Service Affecting (NSA)

The Automatic UPSR Switch Caused by AIS (AUTOSW-AIS) condition indicates that automatic UPSR protection switching occurred because of an AIS condition. If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.18 AUTOSW-LOP (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic UPSR Switch Caused by Loss of Pointer (LOP) condition indicates that automatic UPSR protection switching occurred because of an LOP-P alarm (see page 2-80). If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-81.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.19 AUTOSW-LOP (VTMON)

- Minor (MN), Service Affecting (SA)

The AUTOSW-LOP alarm indicates that automatic UPSR protection switching occurred because of an LOP-V alarm (see page 2-81). If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-LOP (VTMON) Alarm

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-81.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.20 AUTOSW-PDI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic UPSR Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic UPSR protection switching occurred because of a PDI-P alarm (see page 2-93). If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-93.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.21 AUTOSW-SDBER

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic UPSR Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that an SD condition (see page 2-104) caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and reverts to the working path when the SD is resolved.

Procedure: Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.22 AUTOSW-SFBER

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that an SF condition (see page 2-106) condition caused automatic UPSR protection switching to occur. The UPSR is configured for revertive switching and reverts to the working path when the SF is resolved.

Procedure: Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF Condition" procedure on page 2-106.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.23 AUTOSW-UNEQ (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic UPSR Switch Caused by an UNEQ-P alarm (see page 2-122) indicates that an UNEQ alarm caused automatic UPSR protection switching to occur. If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-122.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.24 AUTOSW-UNEQ (VTMON)

- Minor (MN), Service Affecting (SA)

AUTOSW-UNEQ (VTMON) indicates that an UNEQ-V alarm (see page 2-123) caused automatic UPSR protection switching to occur. If the UPSR is configured for revertive switching, it will revert to the working path after the fault clears.

Procedure: Clear the AUTOSW-UNEQ (VTMON) Alarm

Step 1 Complete the "Clear the UNEQ-V Alarm" procedure on page 2-124.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.25 BAT-A-HGH-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The High Voltage Battery (BAT) A condition occurs when the voltage level on battery lead A is between –52 VDC and –56.7 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-A-HGH-VLT Condition

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead A.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.26 BAT-A-LOW-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The Low Voltage Battery A (BAT-A-LOW-VLT) condition occurs when the voltage on battery feed A is low. The low voltage battery A condition occurs when the voltage on battery feed A is between –44 VDC and –40 VDC. The condition clears when voltage remains above this range for 120 seconds.

Procedure: Clear the BAT-A-LOW-VLT Condition

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead A.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.27 BAT-B-HGH-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The High Voltage Battery B (BAT-B-HGH-VLT) condition occurs when the voltage level on battery lead B is between –52 VDC and –56.7 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-B-HGH-VLT Condition

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead B.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.28 BAT-B-LOW-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The Low Voltage Battery B (BAT-B-LOW-VLT) condition occurs when the voltage level on battery lead B is between –44 VDC and –40 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-B-LOW-VLT Condition

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead B.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.29 BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)

The Primary Non-Volatile Backup Memory Failure (BKUPMEMP) alarm refers to a problem with the XTC card’s Flash memory. The alarm occurs when the XTC card is in use and has one of four problems: the Flash manager fails to format a Flash partition; the Flash manager fails to write a file to a Flash partition; there is a problem at the driver level, or the code volume fails the cyclic redundancy check (CRC). CRC is a method to verify for errors in data transmitted to the XTC.

The BKUPMEMP alarm can also cause the EQPT alarm (see page 2-50). If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

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

Procedure: Clear the BKUPMEMP Alarm

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

Step 2 If both XTC cards are powered and enabled, reset the active XTC card to it standby and make the standby XTC card active. Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 3 If the XTC you reset does not reboot 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.30 BLSROSYNC

- Major (MJ), Service Affecting (SA)

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

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Procedure: Clear the BLSROSYNC Alarm

Step 1 Reestablish cabling continuity to the node reporting the alarm.

When the DCC is established between the node and the rest of the BLSR, it becomes visible to the BLSR and should be able to function on the circuits.

Step 2 If alarms occur when you have provisioned the DCCs, see the "EOC" section on page 2-48.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.31 CARLOSS (EQPT)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN Equipment (CARLOSS) alarm occurs when the ONS 15327 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 XTC card. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the ONS 15327.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CARLOSS (EQPT) Alarm

Step 1 Verify connectivity by pinging the ONS 15327 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 15327 IP address]
```

For example, ping 192.1.0.2.

If the workstation has connectivity to the ONS 15327, it shows a "reply from *[IP Address]*" after the ping. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 2 If the ping is successful, an active TCP/IP connection exists. Restart CTC:

a. Exit from CTC.

b. Reopen the browser.

c. Log into CTC.

Step 3 Verify that the straight-through (Category 5) LAN cable is properly connected and attached to the correct port.

Step 4 If the straight-through (Category 5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 5 If you are unable to establish connectivity, replace the straight-through cable with a new known-good cable.

Step 6 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 7 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.32 CARLOSS (E Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the LAN E-series Ethernet (traffic) card is the data equivalent of an LOS (OC-N) alarm (see page 2-84). 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 or an improperly installed Ethernet card. Ethernet card ports must be enabled (in service, IS) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP). The database restoration circumstance applies to the E-series Ethernet cards but not the G1000-2 card, because the G1000-2 card does not use STP and is unaffected by STP reestablishment.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CARLOSS (E-Series) Alarm

Step 1 Verify that the straight-through (Category 5) LAN cable is properly connected and attached to the correct port.

Step 2 If the straight-through (Category 5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to an OC-N card exists, 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 straight-through (Category 5) LAN cable connecting the transmitting device to the Ethernet port.

Step 6 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the Ethernet (traffic) card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the Ethernet (traffic) card.

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

Step 8 If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

Step 9 If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm might 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 the **Select Affected Circuits** dialog box 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 15327 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect:

- Log into the ONS 15327 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. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-128 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15327 Procedure Guide*.

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

2.6.33 CARLOSS (G Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the LAN G-Series Ethernet (traffic) card is the data equivalent of an LOS (OC-N) alarm (see page 2-84). The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-2 card is caused by one of two situations:

- The G1000-2 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 G1000-2 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-2 card), it causes the reporting G1000-2 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 G1000-2 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-2 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 a TPTFAIL (G-Series) alarm (see page 2-120) or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G-Series) alarm.

Refer to the *Cisco ONS 15327 Reference Manual* for a description of the G1000-2 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" section on page 2-120 for more information about alarms that occur when a point-to-point circuit exists between two G1000-2 cards.

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

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CARLOSS (G Series) Alarm

Step 1 Verify that the straight-through (Category 5) LAN cable is properly connected and attached to the correct port.

Step 2 If the straight-through (Category 5) LAN cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 If the alarm does not clear, use an Ethernet test set to determine that a valid signal is coming into the Ethernet port.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 5 If a valid Ethernet signal is not present and the transmitting device is operational, replace the straight-through (Category 5) LAN cable connecting the transmitting device to the Ethernet port.

Step 6 If the alarm does not clear and link autonegotiation is enabled on the G1000-2 port, but the autonegotiation process fails, the G1000-2 turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, verify whether there are conditions that could cause autonegotiation to fail:

a. Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the G1000-2.

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

Step 7 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 8 If the alarm does not clear and a TPTFAIL (G-Series) alarm (see page 2-120) alarm is also reported, complete the "Clear the TPTFAIL (G-Series) Alarm" procedure on page 2-120. 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 might be the G1000-2's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 9 If the TPTFAIL alarm was not reported, verify whether a terminal loopback has been provisioned on the port:

a. In node view, click the card to go to card view.

b. Click the **Conditions** tab and the **Retrieve Conditions** button.

c. If LPBKTERMINAL is listed for the port, a loopback is provisioned. Go to Step 10. If in service (IS) is listed, go to Step 11.

Step 10 If a loopback was provisioned, complete the "Clear a Loopback" procedure on page 2-128.

On the G1000-2 card, provisioning a terminal loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-2 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-2 port detects the termination.

If the does not have a LPBKTERMINAL condition, continue to Step 11.

Step 11 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm might be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect:

Note An Ethernet manual cross-connect is used when another vendors' equipment sits between ONS 15327s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15327 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 the **Select Affected Circuits** dialog box.

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 15327 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect:

- Log into the ONS 15327 at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet (traffic) card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the Type and Size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet (traffic) 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 2-128 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 Procedure Guide* for detailed procedures to create circuits.

Step 12 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130.

Step 13 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the Ethernet (traffic) card.

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

Step 14 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.34 CLDRESTART

- Not Alarmed (NA), (Non-Service Affecting (NSA)

The Cold Restart (CLDRESTART) condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15327 is first powered up.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CLDRESTART Condition

Step 1 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130.

Step 2 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 3 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the card.

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

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.35 COMIOXC

- Critical (CR), Service Affecting (SA)

The Input/Output Slot To XTC Communication Failure (COMIOXC) alarm is caused by a communication error in the XTC card to a high-speed traffic card slot.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the COMIOXC Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 on the reporting XTC card.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting XTC card.

Step 3 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting XTC card.

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

Step 4 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.36 CONTBUS-A-18

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

A Communication Failure from XTC A Slot to XTC Slot alarm occurs when the main processor on the XTC card in Slot 5(termed XTC A) loses communication with the coprocessor on the same card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-A-18 Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the XTC in Slot 6 active.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Position the cursor over the XTC card in Slot 6 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the standby XTC in Slot 5 active.

Step 3 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.37 CONTBUS-B-18

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

A Communication Failure from XTC Slot to XTC slot alarm occurs when the main processor on the XTC card in Slot 6 (termed XTC B) loses communication with the coprocessor on the same card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-B-18 Alarm

Step 1 Position the cursor over the XTC card in Slot 6 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the XTC in Slot 5 active.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Position the cursor over the XTC card in Slot 5 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the standby XTC in Slot 6 active.

Step 3 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.38 CONTBUS-IO-A

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

An XTC A to Shelf Slot Communication Failure alarm occurs when the XTC card in Slot 5 (XTC 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 15327 switches to the standby XTC card. In the case of an XTC protection switch, the alarm clears after the other cards establish communication with the new active XTC card. If the alarm persists, the problem is with the physical path of communication from the XTC to the reporting card. The physical path of communication includes the XTC card, the other card, and the backplane.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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)" section on page 2-90.

Step 2 If the alarm object is any single card slot other then the standby XTC card in Slot 6, perform a CTC reset of the card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-129.

Step 3 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 4 If the alarm object is the standby XTC in Slot 6, perform a soft reset of this card:

a. Right-click the Slot 6 XTC card.

b. Choose **Reset Card** from the shortcut menu.

c. Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 6 If CONTBUS-IO-A is raised on several cards at once, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129. Verify that the card reboots as the standby card.

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 8 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 9 If the reset card or replaced 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.39 CONTBUS-IO-B

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

An XTC B to Shelf Slot Communication Failure alarm occurs when the XTC card in Slot 6 (XTC 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 can appear briefly when the ONS 15327 switches to the standby XTC card. In the case of an XTC protection switch, the alarm clears after the other cards establish communication with the new active XTC card. If the alarm persists, the problem is with the physical path of communication from the XTC to the reporting card. The physical path of communication includes the XTC card, the other card, and the backplane.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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)" section on page 2-90.

Step 2 If the alarm object is any single card slot other then the standby XTC card in Slot 5, perform a CTC reset of the card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-129.

Step 3 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 4 If the alarm object is the standby XTC in Slot 5, perform a soft reset of this card:

a. Right-click the Slot 5 XTC card.

b. Choose **Reset Card** from the shortcut menu.

c. Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 6 If CONTBUS-IO-B is raised on several cards at once, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129. Verify that the card reboots as the standby card.

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 8 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 9 If the reset card or replaced 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.40 CTNEQPT-PBPROT

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect XTC Card Payload Bus (CTNEQPT-PBPROT) alarm indicates a failure of the main payload between the protect XTC card and the reporting traffic card. The XTC card and the reporting card are no longer communicating. The problem exists in the XTC card and the reporting traffic card.

Note If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130 for the standby XTC card. Do not physically reseat an active XTC card. Reseating the XTC disrupts traffic.

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CTNEQPT-PBPROT Alarm

Step 1 Perform a CTC reset on the standby XTC card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-129. (The procedure is the same for the standby XTC as for the traffic card.)

Resetting the standby XTC card will not make it active. Verify that its LED is amber once the reset is complete.

If the cross-connect reset is not complete and error-free or if the XTC reboots automatically, call TAC (1-800-553-2447).

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card.

Step 3 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 will be displayed in the list.

Step 4 If the reporting traffic card is the active card in the protection group, complete the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-127. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 5 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 on the reporting card.

Step 6 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 8 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 9 Complete the "Clear an External Switching Command" procedure on page 2-128.

Step 10 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 11 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the standby cross-connect card.

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

Step 12 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting traffic card.

Step 13 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.41 CTNEQPT-PBWORK

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Working XTC Card Payload Bus (CTNEQPT-PBWORK) alarm indicates a failure in the main payload bus between the active XTC card the reporting traffic card. The XTC card and the reporting card are no longer communicating. The problem exists in the XTC card or the reporting traffic card.

Note If all traffic cards show CTNEQPT-PBWORK alarm, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 for the active XTC card and then complete the "Remove and Reinsert (Reseat) the Standby XTC" procedure on page 3-3. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130 for the XTC card. Do not physically reseat an active XTC card; it disrupts traffic.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CTNEQPT-PBWORK Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 for the active XTC card.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the reporting card.

The reboot takes up to ten minutes.

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card.

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

Step 5 If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-127. If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

Step 6 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the reporting card:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

Step 8 If the CTC reset does not clear the alarm, complete the “Remove and Reinsert (Reseat) a Card” procedure on page 2-130 for the reporting card.

Step 9 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 10 If you switched traffic, complete the “Clear an External Switching Command” procedure on page 2-128.

Step 11 If the alarm does not clear, complete the “Physically Replace a Card” procedure on page 2-130 for the cross-connect card.

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

Step 12 If the alarm does not clear, complete the “Physically Replace a Card” procedure on page 2-130 for the reporting traffic card.

Step 13 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.42 DATAFLT

- Minor (MN), Non-Service Affecting (NSA)

The Software Data Integrity Fault (DATAFLT) alarm occurs when the XTC exceeds its Flash memory capacity.

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

Procedure: Clear the DATAFLT Alarm

Step 1 Complete the “Reset the Active XTC Card in CTC” procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.43 DBOSYNC

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

The Standby Database Out of Synchronization (DBOSYNC) alarm occurs when the standby XTC “To be Active” database does not synchronize with the “Active” database on the active XTC.

Caution If you reset the active XTC while this alarm is raised, you will lose current provisioning.

Procedure: Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active XTC database. Complete the “Back Up the Database” procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change if applying a provisioning change clears the alarm:

a. In node view, click the **Provisioning** > **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 might take up to a minute.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.44 DS3-MISM

- Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-3 Frame Format Mismatch (DS3-MISM) condition indicates a DS-1 frame format mismatch on a signal transiting the XTC-28-3 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type is set to D4 for a DS-1 transiting the XTC-28-3 card, and the incoming signal’s line type format is detected as unframed, then the ONS 15327 reports a DS3-MISM condition.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Note You can only provision DS-1 line frame format on the XTC-28-3 card. DS-3 line format is not provisionable.

Procedure: Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting (active) XTC-28-3 card.

Step 2 Click the **Provisioning** > **DS1** > **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 (ESF, D4, or unframed).

Step 4 If the Line Type drop-down menu does not match the expected incoming signal, select the correct Line Type in the drop-down menu.

Step 5 Click **Apply**.

Step 6 If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the ONS 15327 matches the expected incoming signal.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.45 EHIBATVG-A

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the EHIBATVG-A Alarm

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead A.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.46 EHIBATVG-B

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the EHIBATVG-B Alarm

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead B.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.47 ELWBATVG-A

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the ELWBATVG-A Alarm

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead A.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.48 ELWBATVG-B

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the ELWBATVG-B Alarm

Step 1 The problem is external to the ONS 15327. Troubleshoot the power source supplying battery lead B.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.49 EOC

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

The SONET DCC Termination Failure (EOC) alarm occurs when the ONS 15327 loses its data communications channel. The DCC is three bytes, D1 through D3, in the SONET overhead that convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15327 uses the DCC on the SONET section layer to communicate network management information.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note If a circuit shows an incomplete state when the EOC alarm is raised, it occurs when the logical circuit is in place and 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.

Procedure: Clear the EOC Alarm

Step 1 If an LOS (DS-1) alarm (see page 2-82) is also reported, complete the "Clear the LOS (DS-1) Alarm" procedure on page 2-82.

Step 2 If the alarm does not clear on the reporting node, verify the physical connections between the cards and the fiber-optic cables that are configured to carry DCC traffic.

Step 3 If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service (IS) ports by checking that the ACT LED on each OC-N card is illuminated.

Step 4 If the ACT LEDs on OC-N cards are illuminated, complete the "Verify or Create Node DCC Terminations" procedure on page 2-126 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the OC-N port is active and in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and click **IS** from the drop-down menu. Click **Apply**.

Step 7 If the OC-N card is in service, use an optical test set to verify 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 (traffic) card. It might be necessary to externally switch traffic carrying circuits over to a protection path.

Step 8 If no signal failures on terminations exist, measure power levels to verify that the budget loss is within the parameters of the receiver. See the "Optical Card Transmit and Receive Levels" section on page 1-77.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the "Install the Fiber-Optic Cables" procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

If the alarm clears when the ONS 15327 switches to the standby XTC, the user can assume that the original active XTC is the cause of the alarm.

Step 11 If the XTC replacement does not clear the alarm, delete the problematic DCC termination:

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

b. Highlight the problematic DCC termination.

c. Click **Delete**.

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

Step 12 Recreate the DCC termination using the "Provision SONET DCC Terminations" procedure in the *Cisco ONS 15327 Procedure Guide*.

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 TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.50 EQPT

- Critical (CR), Service Affecting (SA)

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

If the EQPT alarm occurs with a BKUPMEMP alarm, see the "BKUPMEMP" section on page 2-29. The BKUPMEMP procedure also clears the EQPT alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the EQPT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the reporting card:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2 Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 3 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130.

Step 4 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 5 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130.

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

Step 6 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.51 EQPT-MISS

- Critical (CR), Service Affecting (SA)

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the EQPT-MISS Alarm

Step 1 If the alarm is reported against the fan, verify that the fan-tray assembly is present.

Step 2 If the fan-tray assembly is present, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-130.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and complete the "Install the Fan-Tray Assembly" procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.52 E-W-MISMATCH

- Major (MJ), Service Affecting (SA)

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

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

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 1 is west and Slot 4 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.

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

Step 1 Diagram the ring setup, including nodes and spans, on a piece of paper or white board.

Step 2 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 to Node2/Slot6/Port1 (2F BLSR OC48, Ring ID=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/ Port 1.

Step 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.

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.

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

Procedure: 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 Ring ID or Node ID Number" procedure on page 2-125 to identify the node ID, ring ID, and the slot and port in the East Line list and West Line columns. Record the 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 ID and node ID from the information collected in Step 3.

e. Click **Finish** in the BLSR Creation window.

Step 6 Display the node view and click the **Maintenance** > **BLSR** tabs.

Step 7 Change the West Line drop-down menu to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line drop-down menu to the slot you recorded for the West Line in Step 3.

Step 9 Click **OK**.

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

2.6.53 EXCCOL

- Minor (MN), Non-Service Affecting (NSA)

The Excess Collisions on the LAN (EXCCOL) alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15327 and CTC might be affected. The network management LAN is the data network connecting the workstation running the CTC software to the XTC card. The problem causing the alarm is external to the ONS 15327.

Troubleshoot the network management LAN connected to the XTC card for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

Procedure: Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the XTC 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 XTC card and the network management LAN.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.54 EXERCISE-RING-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Exercise Request on Ring (EXERCISE-RING-REQ) condition occurs when optical (traffic) cards in two-fiber BLSRs are tested using the EXERCISE RING command.

Note EXERCISE-RING-REQ is an informational condition. It does not require troubleshooting.

2.6.55 EXERCISE-SPAN-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Exercise Request on Span (EXERCISE-SPAN-REQ) condition occurs when optical (traffic) cards in a BLSR are tested using the EXERCISE SPAN command.

Note EXERCISE-SPAN-REQ is an informational condition. It does not require troubleshooting.

2.6.56 EXT

- Minor (MN), Non-Service Affecting (NSA)

A Failure Detected External to the NE (EXT) alarm occurs because an environmental alarm is present, for example, a door is open or flooding has occurred.

Procedure: Clear the EXT Alarm

Step 1 In node view, click the **Maintenance** tab to gather further information about the EXT alarm.

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.57 EXTRA-TRAF-PREEMPT

- Major (MJ), Service Affecting (SA)

An Extra Traffic Preempted (EXTRA-TRAF-PREEMPT) alarm occurs on OC-N cards in two-fiber BLSRs because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Procedure: Clear the EXTRA-TRAF-PREEMPT Alarm

Step 1 Verify that the protection switch has occurred by checking the Conditions tab.

Step 2 If a ring switch has occurred, clear the alarm on the working system by following the appropriate alarm procedure in this chapter.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.58 FAILTOSW

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Failure to Switch to Protection (FAILTOSW) condition occurs when a working electrical or optical (traffic) card cannot switch to the protect card in a protection group, because another working electrical or optical card with a higher-priority alarm has switched to the protect card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the 1:N electrical card or 1+1 optical card and clears the FAILTOSW.

Step 2 If the condition does not clear, replace the working card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 2-130. This card is the working optical card using the 1+1 protection and not reporting FAILTOSW.

Replacing the working electrical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.

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

Step 3 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.59 FAILTOSW-PATH

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Fail to Switch to Protection Path (FAILTOSW-PATH) condition occurs when the working path does not switch to the protection path on a UPSR. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection card or a lock out set on one of the UPSR nodes.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the FAILTOSW-PATH Condition in a UPSR Configuration

Step 1 Look up and clear the higher priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition.

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 active OC-N card that is reporting the higher priority alarm. Complete the "Physically Replace a Card" procedure on page 2-130. 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 alarm.

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

Step 3 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.60 FAILTOSWR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Fail to Switch to Protection Ring (FAILTOSWR) condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears when one of the following actions occurs: a higher priority event, such as an external switch command occurs, the next ring switch succeeds, or the cause of the APS switch [such as an SD condition (see page 2-104) or an SF condition (see page 2-106)] clears.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the FAILTOSWR Condition in a BLSR Configuration

Step 1 Perform the EXERCISE RING command on the reporting card:

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

b. Click the row of the affected ring under the West Switch column.

c. Select **Exercise Ring** in the drop-down menu.

Step 2 If the condition does not clear, in node view, click **View** > **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 and click the **Maintenance** > **BLSR** tabs.

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

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 6 If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

Step 7 If fiber continuity to the ports is correct, verify that the correct port is in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 8 If the correct port is in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Caution Using an optical test set disrupts service on the optical (traffic) card. It might be necessary to externally 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 15327 Procedure Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-77 lists these specifications.

Step 11 Repeat Steps 6–10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Card" procedure on page 2-130 for the protect standby OC-N card.

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

Step 13 If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.61 FAILTOSWS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Failure to Switch to Protection Span (FAILTOSWS) condition signals an APS span switch failure. FAILTOSWS clears when one of the following actions occur: a higher priority event such as an external switch command occurs; the next span switch succeeds; or an SD condition (see page 2-104) or SF condition (see page 2-106) causing an APS switch clears.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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 menu.

Step 2 If the condition does not clear, in node view, click **View** > **Go to Network View**.

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

Step 4 If clearing other alarms does not clear the FAILTOSWS condition, log into the near-end node and click the **Maintenance** > **BLSR** tabs.

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

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 6 If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

Step 7 If fiber continuity to the ports is correct, verify that the correct port is in service:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 8 If the correct port is in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Caution Using an optical test set disrupts service on the optical (traffic) card. It might 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 15327 Procedure Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-77 lists these specifications.

Step 11 Repeat Steps 6 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Card" procedure on page 2-130 for the protect standby OC-N card.

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

Step 13 If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.62 FAN

- Critical (CR), Service Affecting (SA)

The Fan Failure (FAN) alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15327 can rise above its normal operating range.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the FAN Alarm

Step 1 Verify whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 3-3.

Step 2 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-130.

Note The fan-tray assembly should run immediately when correctly inserted.

Step 3 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 3-1.

Step 4 If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.63 FANDEGRADE

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

The Partial Fan Failure Speed Control Degradation (FANDEGRADE) alarm occurs if fan speed for one of the fans in the fan-tray assembly falls under 500 RPM when read by a tachometry counter.

Procedure: Clear the FANDEGRADE Alarm

Step 1 Complete the "Clear the FAN Alarm" procedure on page 2-60.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.64 FE-AIS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with an LOS (OC-N) alarm (see page 2-84) downstream.

Procedure: Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.65 FE-DS1-MULTLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Multiple DS-1 LOS Detected (FE-DS1-MULTLOS) condition occurs when multiple DS-1 signals are lost at the far-end node.

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 condition or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.66 FE-DS1-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-1 Equipment Failure Non-Service Affecting (FE-DS1-NSA) condition occurs when a far-end XTC 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.67 FE-DS1-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-1 Equipment Failure Service Affecting (FE-DS1-SA) condition occurs when there is a far-end equipment failure on an XTC 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.68 FE-DS1-SNGLLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Single DS-1 LOS(FE-DS1-SNGLLOS) condition occurs when a single DS-1 signal is lost on a far-end XTC card. Signal loss also causes an LOS (OC-N) alarm (see page 2-84).

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SNGLLOS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-SNGLLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.69 FE-DS3-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-3 Equipment Failure Non-Service Affecting (FE-DS3-NSA) condition occurs when a far-end XTC-28-3 card equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS3-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.70 FE-DS3-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-3 Equipment Failure Service Affecting (FE-DS3-SA) condition occurs when there is a far-end equipment failure on an XTC-28-3 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 condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-DS3-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.71 FE-EQPT-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Common Equipment Failure Non-Service Affecting (FE-EQPT-NSA) condition occurs when a non-service affecting equipment failure is detected on a far-end XTC card.

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 condition or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the FE-EQPT-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.72 FE-EXERCISING-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Exercising Ring (FE-EXERCISING-RING) condition occurs when far-end optical (traffic) cards in a two-fiber BLSR are being tested using the EXERCISE RING command. The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-EXERCISING-RING condition.

Note FE-EXERCISING-RING is an informational condition. It does not require troubleshooting.

2.6.73 FE-EXERCISING-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Exercising Span (FE-EXERCISING-SPAN) condition occurs when far-end optical (traffic) cards in a BLSR are being tested using the EXERCISE SPAN command.The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-EXERCISING-SPAN condition.

Note FE-EXERCISING-SPAN is an informational condition. It does not require troubleshooting.

2.6.74 FE-FRCDWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Ring Working Facility Forced to Switch to Protection (FE-FRCDWKSWPR-RING) condition occurs from a far-end node when a ring is forced from working to protect using the FORCE RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. See the "Clear a BLSR Span Lock Out" procedure on page 2-127 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.75 FE-FRCDWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Working Facility Forced to Switch to Protection Span (FE-FRCDWKSWPR-SPAN) condition occurs from a far-end node when a span on a 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-FRCDWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Clear the main alarm. See the "Clear a BLSR Span Lock Out" procedure on page 2-127 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.76 FE-IDLE

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Idle (FE-IDLE) condition occurs when a far-end node detects an idle DS-3 signal.

The prefix FE 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 condition or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Procedure: Clear the FE-IDLE Condition

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Clear the main alarm. Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.77 FE-LOCKOUTOFPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Lock Out of Protection Span (FE-LOCKOUTOFPR-SPAN) condition occurs when a BSLR span is locked out of the protection system from a far-end node using the LOCKOUT 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-LOCKOUTOFPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Make sure there is no lock out set. See the "Clear a BLSR Span Lock Out" procedure on page 2-127 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.78 FE-LOF

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End LOF (FE-LOF) condition occurs when a far-end node reports an LOF (DS-3) alarm (see page 2-79).

The prefix FE 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 condition or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-LOF Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Complete the "Clear the LOF (DS-3) Alarm" procedure on page 2-79. The procedure also applies to FE-LOF.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.79 FE-LOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End LOS (FE-LOS) condition occurs when a far-end node reports an LOS (DS-3) alarm (see page 2-83).

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. Both alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-LOS Condition

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Complete the "Clear the LOF (DS-1) Alarm" procedure on page 2-78.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.80 FE-MANWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Ring Manual Switch of Working Facility to Protect (FE-MANWKSWPR-RING) condition occurs when a BLSR working ring is switched from working to protect at a far-end node using the MANUAL RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-MANWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-MANWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.81 FE-MANWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Manual Switch Span Working Facility to Protect (FE-MANWKSWPR-SPAN) condition occurs when a BLSR span is switched from working to protect at the far-end node using the MANUAL SPAN command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

Procedure: Clear the FE-MANWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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

Step 3 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.82 FEPRLF

- Minor (MN), Non-Service Affecting (NSA)

The Far End Protection Line Failure (FEPRLF) alarm occurs when an APS channel SF condition (see page 2-106) occurs on the protect card coming into the node.

Note The FEPRLF alarm occurs only on the ONS 15327 when bidirectional protection is used on optical (traffic) cards in a 1+1 configuration or BLSR configuration.

Procedure: Clear the FEPRLF Alarm on a BLSR

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.83 FORCED-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch Request on Facility or Equipment (FORCED-REQ) condition occurs when you enter the FORCE command on a span or card to force traffic from a working card or working span to a protection card or protection span or vice versa. You do not need to clear the condition if you want the force switch to remain.

Procedure: Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.84 FORCED-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch Request Ring (FORCED-REQ-RING) condition applies to optical trunk cards when the FORCE RING command is applied to two-fiber BLSRs to move traffic from working to protect.

Procedure: Clear the FORCED-REQ-RING Condition

Step 1 Complete the "Clear the FORCED-REQ Condition" procedure on page 2-69.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.85 FORCED-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch Request Span (FORCED-REQ-SPAN) condition applies to optical trunk cards in BLSRs when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

Procedure: Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear the FORCED-REQ Condition" procedure on page 2-69.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.86 FRCDSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Internal Timing (FRCDSWTOINT) condition occurs when the user issues a Force command to switch to an internal timing source.

Note FRCDSWTOINT is an informational condition. It does not require troubleshooting.

2.6.87 FRCDSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Primary Timing Source (FRCDSWTOPRI) condition occurs when the user issues a Force command to switch to the primary timing source.

Note FRCDSWTOPRI is an informational condition. It does not require troubleshooting.

2.6.88 FRCDSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Second Timing Source (FRCDSWTOSEC) condition occurs when the user issues a Force command to switch to the second timing source.

Note FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

2.6.89 FRCDSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Third Timing Source (FRCDSWTOTHIRD) condition occurs when the user issues a Force command to switch to the third timing source.

Note FRCDSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.6.90 FRNGSYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Free-Running Synchronization Mode (FRNGSYNC) alarm occurs when the reporting ONS 15327 is in free run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the ONS 15327 has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips might begin to occur on an ONS 15327 relying on an internal clock.

Procedure: Clear the FRNGSYNC Alarm

Step 1 If the ONS 15327 is configured to operate from its internal clock, disregard the FRNGSYNC alarm.

Step 2 If the ONS 15327 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.

Step 3 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as a SYNCPRI alarm (see page 2-117) and a SYNCSEC alarm (see page 2-117).

Step 4 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.91 FSTSYNC

- Minor (MN), Non-Service Affecting (NSA)

A Fast Start Synchronization mode (FSTSYNC) alarm occurs when the ONS 15327 is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

Note FSTSYNC is an informational alarm. The alarm does not require troubleshooting.

2.6.92 FULLPASSTHR-BI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Bidirectional Full Pass-Through Active (FULLPASSTHR-BI) condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic, and there is a change in the receive K byte from No Request.

Procedure: Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.93 HITEMP

- Critical (CR), Service Affecting (SA) for NE
- Minor (MN), Non-Service Affecting (NSA) for EQPT

The High Temperature (HITEMP) alarm occurs when the temperature of the ONS 15327 is above 122° F (50° C).

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the HITEMP Alarm

Step 1 Verify that the environmental temperature of the room is not abnormally high.

Step 2 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15327.

Step 3 If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15327 empty slots. Blank faceplates help airflow.

Step 4 If faceplates fill the empty slots, verify whether the air filter needs replacement. Refer to "Inspect and Maintain the Air Filter" procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 5 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-130.

Note The fan-tray assembly should run immediately when correctly inserted.

Step 6 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 3-1.

Step 7 If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447) if the alarm applies to the NE, or a non-service-affecting problem if the alarm applies to equipment.

2.6.94 HLDOVRSYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Holdover Synchronization Mode (HLDOVRSYNC) alarm indicates a loss of the primary or secondary timing reference. Timing reference loss occurs when line coding (AMI, B8ZS) on the timing input is different from the configuration on the ONS 15327. It also usually occurs during the selection of a new node reference clock. The HLDOVRSYNC alarm indicates that the ONS 15327 has gone into holdover and is using the ONS 15327 internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

Procedure: Clear the HLDOVRSYNC Alarm

Step 1 Clear additional alarms that relate to timing, such as a FRNGSYNC condition (see page 2-71); a FSTSYNC condition (see page 2-71); a HLDOVRSYNC alarm (see page 2-73); an LOF (BITS) alarm (see page 2-77); an LOS (BITS) alarm (see page 2-81); a MANSWTOINT condition (see page 2-89); a MANSWTOPRI condition (see page 2-89); a MANSWTOSEC condition (see page 2-89); a MANSWTOTHIRD condition (see page 2-89); a SWTOPRI condition (see page 2-115); a SWTOSEC condition (see page 2-115); a SWTOTHIRD condition (see page 2-115); a SYNC-FREQ condition (see page 2-116); a SYNCPRI alarm (see page 2-117); a SYNCSEC alarm (see page 2-117); or a SYNCTHIRD alarm (see page 2-118).

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.95 IMPROPRMVL

- Critical (CR), Service Affecting (SA)

The Improper Removal (IMPROPRMVL) alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node.

Caution Updating software on a standby XCT card can take up to 30 minutes.

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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

Procedure: 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, take them out of service:

Caution Before taking a port out of service, ensure that no live traffic is present.

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

b. Click the **Provisioning** tab.

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

d. Choose **OOS** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-128.

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 the node view.

b. If you are already in node view, click the **Provisioning** > **Protection** tabs.

c. Click the protection group of the reporting card.

d. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning:

a. Click the **Provisioning** > **SONET DCC** 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 menu for **Ref-1**.

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

d. Click **Apply**.

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

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.96 INC-ISD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-3 Idle (INC-ISD) condition indicates that the XTC-28-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OO-MT state. It is resolved when the OOS state ends.

Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.6.97 INHSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Inhibit Switch To Protect Request on Equipment (INHSWPR) condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1+1 protection scheme, traffic remains locked onto the working system.

Procedure: Clear the INHSWPR Condition

Step 1 Complete the "Clear an External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.98 INHSWWKG

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Inhibit Switch To Working Request on Equipment (INHSWWKG) condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1+1 protection scheme, traffic remains locked onto the protect system.

Procedure: Clear the INHSWWKG Condition

Step 1 Complete the "Clear an External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.99 INVMACADR

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

The Equipment Failure Invalid MAC Address (INVMACADR) alarm occurs when the ONS 15327 MAC Address is invalid. The MAC Address is permanently assigned to the ONS 15327 chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADR. Contact TAC at 1-800-553-2447.

2.6.100 KB-PASSTHR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The K Bytes Pass Through Active (KB-PASSTHR) condition occurs on a non-switching node in a BLSR when the protect channels on the node are not active and the node is in K Byte Pass-Through State.

Procedure: Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.101 LKOUTPR-S

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lock Out of Protection Span (LKOUTPR-S) condition occurs on a BSLR node when traffic is locked out of a protect span using the LOCKOUT SPAN command.

Procedure: Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.102 LOCKOUT-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lock Out Switch Request on Facility/Equipment (LOCKOUT-REQ) condition occurs when a user initiates a lock out switch request for an OC-N card or a lock out switch request on a UPSR at the path level. A lock out prevents protection switching. Clearing the lock out again allows protection switching and clears the LOCKOUT-REQ condition.

Procedure: Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear a UPSR Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.103 LOCKOUT-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lock Out Switch Request Ring (LOCKOUT-REQ-RING) condition occurs when a LOCKOUT RING command is applied to a BLSR to prevent all protection switching on the ring.

Procedure: Clear the LOCKOUT-REQ-RING Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.104 LOF (BITS)

- Major (MJ), Service Affecting (SA)

The Loss of Frame (LOF) BITS alarm occurs when a port on the XTC BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15327 has lost frame delineation in the incoming data.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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

Procedure: Clear the LOF (BITS) Alarm

Step 1 Verify that the framing and line coding match between the BITS input and the XTC:

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

b. Find the framing and coding 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 the Coding field matches the coding of the BITS timing source (B8ZS or AMI).

e. If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down menu.

f. Verify that the Framing field matches the framing of the BITS timing source, either SF (D4) or ESF.

g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down menu.

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

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the XTC, complete the "Physically Replace a Card" procedure on page 2-130 for the XTC card.

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

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.105 LOF (DS-1)

- Major (MJ), Service Affecting (SA)

The DS-1 LOF alarm indicates that the receiving ONS 15327 has lost frame delineation in an incoming DS-1 data stream.

Procedure: Clear the LOF (DS-1) Alarm

Step 1 Verify that the line framing and line coding match between the DS-1 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 XTC.

d. Click the **Provisioning** > **DS1** > **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 menu and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source's line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the Line Coding cell and choose the right type from the drop-down menu.

g. If the signal source line coding does not match the reporting port, click the **Line Coding** column and choose the appropriate type from the drop-down menu.

h. Click **Apply**.

Note On the DS-1 Line tab, the B8ZS coding field is normally paired with ESF in the Line Type field. AMI coding is normally paired with D4 in the Line Type field.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.106 LOF (DS-3)

- Critical (CR), Service Affecting (SA)

The DS-3 LOF alarm indicates that the receiving ONS 15327 has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment might be set to a format that differs from the receiving ONS 15327. On XTC-28-3 cards, the alarm occurs only on DS-1 lines with the provisionable framing format set to SF (D4) and not on cards with the provisionable framing format set to unframed.

Procedure: Clear the LOF (DS-3) Alarm

Step 1 Change the line type of the non-ONS equipment attached to the reporting card to D4:

a. Display the card view of the reporting card.

b. Click the **Provisioning > DS1 > 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 **D4** from the drop-down menu.

e. Click **Apply**.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.107 LOF (OC-N)

- Critical (CR), Service Affecting (SA)

The OC-N LOF alarm occurs when a port on the reporting OC-N card has an LOF condition. LOF indicates that the receiving ONS 15327 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

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

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the LOF (OC-N) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Step 2 If cabling continuity is correct, clean the fiber connectors according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 3 If the alarm does not clear, see the "Network Troubleshooting Tests" section on page 1-2 to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call TAC to report a service-affecting problem (1-800-553-2447).

2.6.108 LOP-P

- Critical (CR), Service Affecting (SA)

A Loss of Pointer Path (LOP-P) alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the LOP-P Alarm

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify that the correct circuit size is listed in the Size column. If the size is different from what is expected, such as an STS 3c instead of an STS1, this will cause the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.

Step 4 If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-128.

Step 5 Recreate the circuit for the correct size. For instructions, see the *Cisco ONS 15327 Procedure Guide*.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.109 LOP-V

- Major (MJ), Service Affecting (SA)

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.

Procedure: Clear the LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-81.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.110 LOS (BITS)

- Major (MJ), Service Affecting

The BITS LOS alarm indicates that the XTC card has an LOS from the BITS timing source. The LOS (BITS-N) means that 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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15327 MIC to the timing source.

Step 2 If wiring is correct, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.111 LOS (DS-1)

- Major (MJ), Service Affecting (SA)

A DS-1 LOS alarm for a DS-3 port or a DS-1 port occurs when the XTC port 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.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the LOS (DS-1) Alarm

Step 1 Verify cabling continuity to the port.

Step 2 If the cabling is correct, verify that the correct port is in service (IS):

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 4 If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 5 If a valid signal exists, replace the DS-N connector on the MIC card.

Step 6 Repeat Steps 1 through 5 for any other port on the card that reports the LOS.

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8 If no other alarms are present that might be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.112 LOS (DS-3)

- Critical (CR), Service Affecting (SA)

The DS-3 LOS alarm for either an XTC DS-3 port or 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. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place and will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Procedure: Clear the LOS (DS-3) Alarm

Step 1 Verify cabling continuity to the port.

Step 2 If the cabling is correct, verify that the correct port is in service (IS):

Step 3 Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

f. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

h. Verify that the **State** column lists the port as IS.

i. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 4 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 5 If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 6 If a valid signal exists, replace the DS-N connector on the MIC card.

Step 7 Repeat Steps 1 through 5 for any other port on the card that reports the LOS.

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 9 If no other alarms exist that might be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

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

2.6.113 LOS (OC-N)

- Critical (CR), Service Affecting (SA)

An OC-N LOS alarm 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 **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place and will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Procedure: Clear the LOS (OC-N) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is correct, verify that the correct port is in service.

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card:

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber connectors according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-77 lists these specifications for each card.

Step 5 If optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 6 Repeat Steps 1 through 5 for any other port on the card reporting the alarm.

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8 If no other alarms exist that might be the source of the LOS, or if clearing an alarm did not clear the LOS (OC-N), complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.114 LPBKCRS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Loopback XTC (LPBKCRS) condition indicates that there is a software cross-connect loopback active between a traffic card and an XTC card. A cross-connect loopback is a sub-line speed test that does not affect traffic.

For more information on loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-4.

Clear the LBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the traffic card in CTC to display the card view.

Step 2 Click the **Provisioning** > **SONET STS** tabs.

Step 3 Under the **XC Loopback** column, deselect the check box for the port.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (TAC) at 1-800-553-2447.

2.6.115 LPBKFACILITY (DS-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A DS-N Loopback Facility (LPBKFACILITY) condition occurs when a software facility loopback is active for a port on the reporting card. For more information about loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-4.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Note XTC-28-3 cards only support facility loopbacks on DS-1 circuits.

Procedure: Clear the LPBKFACILITY (DS-N) Condition

Step 1 From the node view, double-click the reporting XTC-28-3 card to display the card view.

Step 2 Click the **Maintenance** > **DS3** tab.

If the condition is reported against a DS-1 line, also click the **DS1** tab.

Step 3 Complete the "Clear a Loopback" procedure on page 2-128.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.116 LPBKFACILITY (OC-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

An OC-N Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

For more information about loopbacks, see the "Identify Points of Failure on an OC-N Circuit Path" section on page 1-21.

Procedure: Clear the LPBKFACILITY (OC-N) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

Caution Before performing a facility loopback on an OC-N card, make sure the card contains at least two DCC paths to the node where the card is installed. A second DCC 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 15327 containing the loopback OC-N.

2.6.117 LPBKTERMINAL (DS-N, OC-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A DS-N or OC-N Loopback Terminal (LPBKTERMINAL) condition occurs when a software facility loopback is active for a port on the reporting card.

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

Note Terminal loopback is not supported at the DS1 level for the XTC-28-3 card.

Procedure: Clear the LPBKTERMINAL (DS-N, OC-N) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.118 LPBKTERMINAL (G-Series)

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

When a port in terminal loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-2 card, the outgoing signal is not transmitted; it is only redirected in the receive direction. G1000-2 cards only support terminal loopbacks.

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

Procedure: Clear the LPBKTERMINAL (G-Series) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-128.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.119 MAN-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

Procedure: Clear the MAN-REQ Condition

Step 1 Complete the "Clear a UPSR Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.120 MANRESET

- Not Alarmed (NA), Non-Service Affecting (NSA)

A User-Initiated Manual Reset (MANRESET) condition occurs when you right-click a card in CTC and choose **Reset**. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

Note MANRESET is an informational condition. It does not require troubleshooting.

2.6.121 MANSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Internal Clock (MANSWTOINT) condition occurs when the NE timing source is manually switched to the internal timing source.

Note MANSWTOINT is an informational condition. It does not require troubleshooting.

2.6.122 MANSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Primary Reference (MANSWTOPRI) condition occurs when the NE timing source is manually switched to the primary timing source.

Note MANSWTOPRI is an informational condition. It does not require troubleshooting.

2.6.123 MANSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Second Reference (MANSWTOSEC) condition occurs when the NE timing source is manually switched to the second timing source.

Note MANSWTOSEC is an informational condition. It does not require troubleshooting.

2.6.124 MANSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Third Reference (MANSWTOTHIRD) condition occurs when the NE timing source is manually switched to the tertiary timing source.

Note MANSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.6.125 MANUAL-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch Request on Ring (MANUAL-REQ-RING) condition occurs when a user initiates a MANUAL RING command on two-fiber BLSR rings to switch from working to protect or protect to working.

Procedure: Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.126 MANUAL-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch Request on Span (MANUAL-REQ-SPAN) condition occurs on BLSRs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span.

Procedure: Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.127 MEA (EQPT)

- Critical (CR), Service Affecting (SA)

The Missing Equipment Attributes (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. Removing the incompatible cards clears the alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that sits in the slot reported in the Alarms window MEA alarm Object column.

Step 2 In CTC, click the **Inventory** tab to reveal the provisioned card type.

Step 3 If you prefer the card type depicted by CTC, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

Step 4 If you prefer the card that physically occupies the slot and the card is not in service, has no circuits mapped, 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, 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 5 If any ports on the card are in service, take them out of service:

Caution Before taking ports out of service, ensure that no live traffic.

a. Double-click the reporting card to display the card view:

b. Click the **Provisioning** tab.

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

d. Choose **OOS** to take the ports out of service.

Step 6 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-128.:

Caution Before deleting the circuit, ensure that live traffic is not present.

Step 7 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 8 Right-click the card reporting the alarm.

Step 9 Choose **Delete**.

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

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

2.6.128 MEM-GONE

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

The Memory Gone (MEM-GONE) alarm occurs when data generated by software operations exceeds the memory capacity of the XTC card. CTC and the XTC card do not function properly until the alarm clears. The alarm clears when additional memory becomes available.

The alarm does not require user intervention. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.129 MEM-LOW

- Minor (MN), Non-Service Affecting (NSA)

The Free Memory of Card Almost Gone (MEM-LOW) alarm occurs when data generated by software operations is close to exceeding the memory capacity of the XTC card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the XTC card is exceeded, CTC ceases to function.

The alarm does not require user intervention. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.130 MFGMEM

- Critical (CR), Service Affecting (SA)

The Manufacturing Data Memory Failure (MFGMEM) alarm occurs if the ONS 15327 cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the XTC lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. An inability to read a valid MAC address disrupts IP connectivity and grays out the ONS 15327 icon on the CTC network view.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the MFGMEM (BP, Fan-Tray Assembly) Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

Step 3 If the MFGMEM alarm continues to report after replacing the XTC cards, the problem is with the EEPROM.

Step 4 If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 3-1.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.131 PDI-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

The ONS 15327 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS condition (see page 2-16) often accompanies the PDI-P condition. If the PDI-P is the only condition reported with the AIS condition (see page 2-16), clear the PDI-P condition to clear the AIS condition. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on the port of an OC-N card supporting a G1000-2 card circuit might result from the end-to-end Ethernet link integrity feature of the G1000-2. If the link integrity is the cause, it typically is accompanied by an a TPTFAIL (G-Series) alarm (see page 2-120) or a CARLOSS (G Series) alarm (see page 2-33) reported against one or both Ethernet ports terminating the circuit. If TPTFAIL or CARLOSS are reported against one or both of the Ethernet ports, troubleshooting the accompanying alarm clears the PDI-P condition.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the PDI-P Condition

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

a. Click the **Circuits** tab.

b. Verify that the **State** column lists the port as active.

c. If the State column lists the port as incomplete, wait up to ten minutes for the ONS 15327 to initialize fully. If the incomplete state does not change after full initialization, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

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

Step 3 If traffic is affected, complete the "Delete a Circuit" procedure on page 2-128.

Caution Deleting a circuit might affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 Procedure Guide* for detailed procedures to create circuits.

Step 5 If circuit deletion and recreation does not clear the condition, verify that the far-end OC-N card providing STS payload to the reporting card is not errored.

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 15327 Procedure Guide*.

Step 8 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the optical/electrical cards.

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

Step 9 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.132 PEER-NORESPONSE

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

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

Procedure: Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the protect card:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" (loading) appears on the reset card in CTC.

Step 2 Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the working card:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 4 Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.133 PLM-P

- Critical (CR), Service Affecting (SA)

A Payload Label Mismatch Path (PLM-P) alarm indicates that signal does not match its label. The condition occurs due to an invalid C2 byte value in the SONET path overhead.

For example, this alarm can occur when a card is expecting a 0 value in the C2 byte, but receives a 4 instead. This can occur on the XTC card when the card expects a DS-1 signal but receives a DS-3 signal. The DS-3 signal C2 byte value is 4, so this will cause a label mismatch and a PLM-P alarm.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the PLM-P Alarm

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

a. Click the **Circuits** tab.

b. Verify that the **State** column lists the port as active.

c. If the State column lists the port as incomplete, wait up to ten minutes for the ONS 15327 to initialize fully. If the incomplete state does not change after full initialization, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

Step 2 After determining the port is active, verify the signal source to the traffic card reporting the alarm with an optical test set according to site specific practice.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If traffic is being affected, complete the "Delete a Circuit" procedure on page 2-128.

Caution Deleting a circuit might affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 Procedure Guide* for detailed procedures to create circuits.

Step 5 If the circuit deletion and recreation does not clear the alarm, verify the far-end OC-N card that provides STS payload to the XTC card.

Step 6 If the alarm does not clear, verify the cross-connect between the OC-N card and the XTC card.

Step 7 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 15327 Procedure Guide*.

Step 8 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting traffic card.

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

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.134 PLM-V

- Minor (MN), Service Affecting (SA)

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

Procedure: Clear the PLM-V Alarm

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

Step 2 If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.135 PRC-DUPID

- Major (MJ), Service Affecting (SA) for Ring
- Major (MJ), Non-Service Affecting (NSA) for NE

The Procedural Error Duplicate Node ID (PRC-DUPID) alarm indicates that two identical node IDs exist in the same ring. The ONS 15327 requires each node in the ring to have a unique node ID.

Procedure: Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a Ring ID or Node ID Number" procedure on page 2-125.

Step 3 Repeat Step 2 for all the nodes on the ring.

Step 4 If two nodes have an identical node ID number, complete the "Change a Node ID Number" procedure on page 2-126 so that each node ID is unique.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.136 PROTNA

- Minor (MN), Non-Service Affecting (NSA)

The Protection Unit Not Available (PROTNA) alarm is caused by an OOS or failed protection card when an XTC that is provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if the alarm is raised against an XTC, ensure that there is a redundant control card installed and provisioned in the chassis.

Step 2 If the alarm is raised against a traffic card, verify whether the ports have been taken out of service:

a. In CTC, double-click the reporting card to display the card view (if the card is not a cross-connect card).

b. Click the **Provisioning** tab.

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

d. Choose **OOS** to take the ports out of service.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the reporting card:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 4 Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 6 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.

- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 7 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.137 PWR-A

- Minor (MN), Non-Service Affecting (NSA)

An NE Power Failure at Connector A alarm indicates that the power is out of the specified 48 VDC input range and is either too high (overvoltage) or too low (undervoltage), requiring you to check the incoming power feed or separate power distribution equipment, or both. The PWR-A alarm may also be raised before actual loss of power in a discharging power plant problem and before full loss of incoming power.

Overvoltage or undervoltage can be caused by incoming DC power problems such as power rectifier failure, faulty power cabling, or a blown fuse.

Cisco encourages the use of separate DC power feeds from separate DC power plants or AC power rectifiers to ensure power redundancy to the feeds. Using a single DC power source for both MIC-A/PWR-A and MIC-B/PWR-B creates a risk through the single point of possible failure. Using dual power feeds removes this risk liability.

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

Procedure: Clear the PWR-A Alarm

Step 1 Determine whether the PWR-A alarm is occurring alone or in conjunction with the PWR-B alarm, and determine whether MIC A and MIC B are using one single or two separate power supplies.

Step 2 If you are using separate power sources for the MIC A and MIC B power connectors and the PWR-A alarm occurs without the PWR-B alarm, inspect the incoming voltage to the MIC A connector using site practices. The alarm can be caused by problems such as power rectifier failure, faulty power cabling, or a blown fuse, and correct these issues. Solve these problems before continuing.

You can verify the power connection continuity and the power source output with a voltmeter using the procedures in the *Cisco ONS 15327 Procedure Guide*.

Step 3 If you are using a single power source for both the MIC A and MIC B cards and only the PWR-A alarm is occurring, an electrical cable continuity or connection problem may be to blame. Check for these problems and correct them if necessary.

Step 4 If you are using separate power sources for each MIC card and the PWR-A alarm occurs in conjunction with the PWR-B alarm, it is likely that both incoming power feeds or power plants are failing. Check for these problems according to site practice and correct as necessary.

Step 5 If you are using a single power source for both MIC cards and both the PWR-A and PWR-B alarms are raised, problems with both power feeds may be to blame, but a power plant failure is more likely. Check for these problems according to site practice and correct as necessary.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.138 PWR-B

- Minor (MN), Non-Service Affecting (NSA)

An NE Power Failure at Connector B alarm indicates that the power is out of the specified 48 VDC input range and is either too high (overvoltage) or too low (undervoltage), requiring you to check the incoming power feed or separate power distribution equipment, or both. The PWR-B alarm may also be raised before actual loss of power in a discharging power plant problem and before full loss of incoming power.

Overvoltage or undervoltage can be caused by incoming DC power problems such as power rectifier failure, faulty power cabling, or a blown fuse.

Cisco encourages the use of separate DC power feeds from separate DC power plants or AC power rectifiers to ensure power redundancy to the feeds. Using a single DC power source for both MIC-A/PWR-A and MIC-B/PWR-B creates a risk through the single point of possible failure. Using dual power feeds removes this risk liability.

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

Procedure: Clear the PWR-B Alarm

Step 1 Determine whether the PWR-B alarm is occurring alone or in conjunction with the PWR-A alarm, and determine whether MIC A and MIC B are using one single or two separate power supplies.

Step 2 If you are using separate power sources for the MIC A and MIC B power connectors and the PWR-B alarm occurs without the PWR-A alarm, inspect the incoming voltage to the MIC B connector using site practices. The alarm can be caused by problems such as power rectifier failure, faulty power cabling, or a blown fuse, and correct these issues. Solve these problems before continuing.

You can verify the power connection continuity and the power source output with a voltmeter using the procedures in the *Cisco ONS 15327 Procedure Guide*.

Step 3 If you are using a single power source for both the MIC A and MIC B cards and only the PWR-B alarm is occurring, an electrical cable continuity or connection problem may be to blame. Check for these problems and correct them if necessary.

Step 4 If you are using separate power sources for each MIC card and the PWR-B alarm occurs in conjunction with the PWR-A alarm, it is likely that both incoming power feeds or power plants are failing. Check for these problems according to site practice and correct as necessary.

Step 5 If you are using a single power source for both MIC cards and both the PWR-A and PWR-B alarms are raised, problems with both power feeds may be to blame, but a power plant failure is more likely. Check for these problems according to site practice and correct as necessary.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.139 PWR-REDUN

- Minor (MN), Non-Service Affecting (NSA)

The Redundant Power Capability Lost (PWR-REDUN) alarm applies to cards that have two built-in fuses (such as newer optical cards). The alarm indicates that one of the fuses has blown and must be serviced. When this alarm occurs, the card's power redundancy is lost because only one card power connection can contact one of the redundant power supplies.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the PWR-REDUN Alarm

Step 1 The card fuse is not field-replaceable. Complete the "Physically Replace a Card" procedure on page 2-130.

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

Step 2 Log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447) to arrange a card return for service.

2.6.140 RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Remote Alarm Indication (RAI) condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on the DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS condition (see page 2-16).

Procedure: Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.141 RCVR-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Receiver Missing (RCVR-MISS) alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its connector. Incorrect impedance usually occurs when a receive cable is missing from the XTC DS-1 port or a possible mismatch of equipment occurs.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the RCVR-MISS Alarm

Step 1 Ensure that the device attached to the XTC port is operational.

Step 2 If the attachment is correct, verify that the cabling is securely connected.

Step 3 If the cabling is correct, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the receive cable.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.142 RFI-L

- Not Reported (NR), Non-Service Affecting (NSA)

A Remote Fault Indication (RFI) Line condition occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Procedure: Clear the RFI-L Condition

Step 1 Log into the node at the far-end node of the reporting ONS 15327.

Step 2 Verify whether there are other alarms, especially an LOS (OC-N) alarm (see page 2-84).

Step 3 Clear the alarms; to clear an LOS (OC-N) alarm (see page 2-84), refer to the LOS section in this chapter.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.143 RFI-P

- Not Reported (NR), Non-Service Affecting (NSA)

An RFI Path condition occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the node that terminates a path.

Procedure: Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS) on the reporting ONS 15327:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

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

Step 3 Clear alarms in the node with the failure, especially an UNEQ-P alarm (see page 2-122) or an UNEQ-V alarm (see page 2-123).

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.144 RFI-V

- Not Reported (NR), Non-Service Affecting (NSA)

An RFI VT Layer condition occurs when the ONS 15327detects 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.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

⚠ **Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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 15327 Procedure Guide*.

Step 2 If connectors are correctly connected, verify that the XTC port is active and in service (IS):

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as IS.

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 3 If the ports are active and in service, use an optical test set to verify whether the signal source has 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 15327.

Step 5 Clear alarms in the far-end node, especially an UNEQ-P alarm (see page 2-122) or an UNEQ-V alarm (see page 2-123).

Step 6 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.145 RING-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Mismatch Ring (RING-MISMATCH) alarm occurs when the ring ID of the ONS 15327 that is reporting the alarm does not match the ring ID of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical ring IDs to function.

Procedure: Clear the RING-MISMATCH Alarm

Step 1 In node view, click the **Provisioning** > **BLSR** tabs.

Step 2 Note the number in the Ring ID field.

Step 3 Log into the next ONS node in the BLSR.

Step 4 Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-125.

Step 5 If the ring ID matches the ring ID in the reporting ONS node, repeat Step 4 for the next ONS node in the BLSR.

Step 6 Complete the "Change a Ring ID Number" procedure on page 2-125.

Step 7 Verify that the ring map is correct.

Step 8 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.146 RING-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Switch is Active East Side (RING-SW-EAST) condition occurs when a ring switch occurs at the east side of two-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.147 RING-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Switch is Active West Side (RING-SW-WEST) condition occurs when a ring switch occurs at the west side of a two-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-WEST is an informational condition. It does not require troubleshooting.

2.6.148 SD

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

The BER threshold on the ONS 15327 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}.

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

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the 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.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the SD Condition

Step 1 Complete the "Verify BER Threshold Level" procedure on page 2-129.

Step 2 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure the level is within guidelines.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If the optical power level is correct, verify that optical receive levels are within the acceptable range.

Step 4 If receive levels are correct, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 5 If the alarm does not clear, verify that single-mode fiber is used.

Step 6 If the fiber is the correct type, verify that a single-mode laser is used at the far-end node.

Step 7 If the problem does not clear, the transmitter at the other end of the optical line might be failing and require replacement.

Step 8 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.149 SD-L

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SD Line condition is similar to an SD condition (see page 2-104). It applies to the line level of the SONET signal.

Procedure: Clear the SD-L Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.150 SD-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SD Path (SD-P) condition is similar to an SD condition (see page 2-104) 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 UPSR protected circuits, the BER threshold on the ONS 15327 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6}.

On UPSR, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR 1+1 or 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 bit error rate 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.

Procedure: Clear the SD-P Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.151 SF

- Not Alarmed (NA), Non-Service Affecting (NSA)

A Signal Fail (SF) condition occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure threshold. Signal failure is defined by Telcordia as a "hard failure" condition. The SD condition (see page 2-104) and SF both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold on the ONS 15327 is user provisionable and has a range for SF from 10-5 to 10-3.

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

SF causes a card to switch from working to protect at either the path or line level. The SF 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.

Procedure: Clear the SF Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.152 SF-L

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SF Line (SF-L) condition is similar to an SF condition (see page 2-106) but it applies to the line layer of the signal.

Procedure: Clear the SF-L Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.153 SF-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SF Path (SF-P) condition is similar to an SF condition (see page 2-106), 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 UPSR circuits, the BER threshold on the ONS 15327 is user provisionable and has a range for SF from 10^{-5} to 10^{-3}. For BLSR 1+1 or unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-3}.

For UPSR, SF-P causes a switch from the working card to the protect card at the path (STS) level. For BLSR 1+1 or unprotected circuits, SF-P 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.

Procedure: Clear the SF-P Condition

Step 1 Complete the "Clear the SD Condition" procedure on page 2-105.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.154 SFTWDOWN

- Minor (MN), Non-Service Affecting (NSA)

A Software Download in Progress (SFTWDOWN) alarm occurs when the XTC is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

⚠ **Caution** It can take up to 30 minutes for software to be updated on a standby XTC card.

Note SFTWDOWN is an informational alarm.

2.6.155 SNTP-HOST

- Minor (MN), Non-Service Affecting (NSA)

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

Procedure: Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which might affect the SNTP server/router connecting to the proxy ONS 15327.

Step 3 If no network problems exist, ensure that the ONS 15327 proxy is provisioned correctly:

a. In node view for the ONS node serving as the proxy, click the **Provisioning** > **General** tabs.

b. Ensure that the Use NTP/SNTP Server check box is checked.

c. If the Use NTP/SNTP Server check box is not checked, click the box.

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 15327 Reference Manual* for more information about SNTP host.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.156 SPAN-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Span Switch is Active East Side (SPAN-SW-EAST) condition occurs when a span switch occurs at the east side of a BLSR span. The condition clears when the switch is cleared.

Note SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.157 SPAN-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Span Switch is Active West Side (SPAN-SW-WEST) condition occurs when a span switch occurs at the west side of a BLSR span. The condition clears when the switch is cleared.

Note SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.158 SQUELCH

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Squelching Traffic (SQUELCH) condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The AIS-P condition (see page 2-17) also appears on all nodes in the ring except the isolated node.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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 correct, verify that the proper ports are in service (IS):

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

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

d. Verify that the **State** column lists the port as in service (IS).

e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 4 If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 5 If the signal is valid, verify that the power level of the optical signal is within the optical card's receiver specifications. Refer to the *Cisco ONS 15327 Reference Manual* for card specifications.

Step 6 If the receiver levels are correct, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are correct, complete the "Physically Replace a Card" procedure on page 2-130 for the OC-N card.

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

Step 8 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.159 SSM-DUS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Status Message (SSM) Quality Changed to Do-Not-Use (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. It does not require troubleshooting.

2.6.160 SSM-FAIL

- Minor (MN), Non-Service Affecting (NSA)

The SSM Failed (SSM-FAIL) alarm occurs when the synchronization status messaging received by the ONS 15327 fails. The problem is external to ONS 15327. The ONS 15327 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

Procedure: Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM.

For specific procedures to use the test set equipment, consult the manufacturer.

If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.161 SSM-LNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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 LNC-quality.

Note SSM-LNC is an informational condition. It does not require troubleshooting.

2.6.162 SSM-OFF

- Not Alarmed (NA), Non-Service Affecting (NSA)

The SSM Off (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 15327 is set up to receive SSM, but the timing source is not delivering SSM messages.

Procedure: Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-110.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.163 SSM-PRC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level is changed to PRC-quality.

Note SSM-PRC is an informational condition. It does not require troubleshooting.

2.6.164 SSM-PRS

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.165 SSM-RES

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.166 SSM-SMC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.167 SSM-ST2

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.168 SSM-ST3

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.169 SSM-ST3E

- Not Alarmed (NA), Non-Service Affecting (NSA)

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 not used for Generation 1.

Note SSM-ST3E is an informational condition. It does not require troubleshooting.

2.6.170 SSM-ST4

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.171 SSM-STU

- Not Alarmed (NA), Non-Service Affecting (NSA)

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 15327 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 15327.

Procedure: Clear the STU Condition

Step 1 In node view, click the **Provisioning** > **Timing** tabs.

Step 2 If **Sync Messaging** is checked, deselect the box.

Step 3 If **Sync Messaging** is unchecked, check the box.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.172 SSM-TNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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. It does not require troubleshooting.

2.6.173 SWMTXMOD

- Critical (CR), Service Affecting (SA)

The Switching Matrix Module Failure (SWMTXMOD) alarm occurs on the XTC card or a traffic card. If the alarm reports against a traffic card, it occurs when the logic component on the XTC card is out of frame (OOF) with the logic component on the reporting traffic card. All traffic on the reporting traffic card is lost.

If the alarm reports against an XTC card, it occurs when a logic component internal to the reporting XTC card is out of frame with a second logic component on the same XTC card. One or more traffic cards might lose traffic as a result of the cross-connect frame failure.

Note The only way to switch the XTC protection group is to reset the active XTC.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the SWMTXMOD Alarm

Step 1 If the card reporting the alarm is the standby cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the card.

Step 2 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby cross-connect card.

Note After the active cross-connect goes into standby, the original standby slot becomes active. The former standby card ACT/STBY LED becomes green.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card.

The reboot takes up to ten minutes.

Step 6 Complete the "Reset a Traffic Card in CTC" procedure on page 2-129 for the reporting card:

- While the card resets, the FAIL LED on the physical card node blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

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

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15327, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15327, an amber LED depiction with “Sby” has replaced the white “LDG” depiction on the card in CTC.

Step 8 If the alarm does not clear, complete the “Remove and Reinsert (Reseat) a Card” procedure on page 2-130 for the traffic card.

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.174 SWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Switch to Primary Reference (SWTOPRI) condition occurs when the ONS 15327 switches to the primary timing source (reference 1). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Note SWTOPRI is an informational condition. It does not require troubleshooting.

2.6.175 SWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Switch to Secondary Reference (SWTOSEC) condition occurs when the ONS 15327 has switched to the secondary timing source (reference 2). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI alarm (see page 2-117).

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.176 SWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Switch to Third Reference (SWTOTHIRD) condition occurs when the ONS 15327 has switched to the third timing source (reference 3). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Procedure: Clear the SWTOTHIRD Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as a SYNCPRI alarm (see page 2-117) or a SYNCSEC alarm (see page 2-117).

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.177 SYNC-FREQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Reference Frequency Out Of Bounds (SYNC-FREQ) condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: 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 timing falls within the proper frequency.

For specific procedures to use the test set equipment, consult the manufacturer. For BITS, the proper timing frequency range is approximately –15 ppm to 15 ppm. For optical line timing, the proper frequency range is approximately –16 ppm to 16 ppm.

Step 2 If the reference source frequency is not outside of bounds, complete the "Physically Replace a Card" procedure on page 2-130 for the XTC card.

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

Note The active XTC takes up to 30 minutes to transfer the system software to the newly installed XTC. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the XTC flash fail and then the active/standby LED flashes. When the transfer completes, the XTC reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ alarm continues to report after replacing the XTC card, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.178 SYNCPRI

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Primary Reference (SYNCPRI) alarm occurs when the ONS 15327 loses the primary timing source (reference 1). The ONS 15327 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 15327 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers a SWTOSEC condition (see page 2-115).

Procedure: Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning** > **Timing** tabs.

Step 2 Verify the current configuration for the REF-1 of the NE Reference.

Step 3 If the primary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 If the primary reference clock is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

Step 5 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.179 SYNCSEC

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Secondary Reference (SYNCSEC) alarm occurs when the ONS 15327 loses the secondary timing source (reference 2). The ONS 15327 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 15327 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15327. Switching to the third timing source also triggers a SWTOTHIRD condition (see page 2-115).

Procedure: Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning** > **Timing** tabs.

Step 2 Verify the current configuration of the REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

Step 6 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.180 SYNCTHIRD

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Third Reference (SYNCTHIRD) alarm occurs when the ONS 15327 loses the third timing source (reference 3). The ONS 15327 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 15327 uses an internal reference for source three, the XTC card might have failed. The ONS 15327 often reports either a FRNGSYNC condition (see page 2-71) or a HLDOVRSYNC alarm (see page 2-73) after a SYNCTHIRD alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning** > **Timing** tabs.

Step 2 Verify the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15327 Procedure Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 If the third timing source is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

Step 5 If the third timing source uses the internal ONS 15327 timing, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.181 SYSBOOT

- Major (MJ), Service Affecting (SA)

The System Reboot (SYSBOOT) alarm indicates that new software is booting on the XTC card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 10 minutes if the same version of software is present on both cards, or up to 30 minutes if the software is being updated from one XTC to the other.

If it does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.6.182 TIM-P

- Critical (CR), Service Affecting (SA) for STSTERM
- Minor (MN), Non-Service Affecting (NSA) for STSMON

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

In manual mode at the Path Trace window, the user types the expected string into the 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 an LOS (OC-N) alarm (see page 2-84), an UNEQ-P alarm (see page 2-122), or a PLM-P alarm (see page 2-95). If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

Procedure: Clear the TIM-P Alarm

Step 1 Log into the circuit source node and click the **Circuits** tab.

Step 2 Select the circuit reporting the alarm, then click **Edit**.

Step 3 In the Edit Circuit window, check the **Show Detailed Map** check box.

Step 4 On the detailed circuit map, right-click the source circuit port and choose **Edit J1 Path Trace** from the shortcut menu.

Step 5 On the detailed circuit map, right-click the drop/destination circuit port and choose **Edit Path Trace** from the shortcut menu.

Step 6 Compare the Current Transmit String and the Current Expected String entries in the Edit J1 Path Trace dialog box.

Step 7 If the strings differ, correct the Transmit or Expected strings and click **Apply**.

Step 8 Click **Close**.

Step 9 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.183 TPTFAIL (G-Series)

- Major (MJ), Service Affecting (SA)

The Transport (TPT) Layer Failure alarm for the G-series Ethernet (traffic) cards indicates a break in the end-to-end Ethernet link integrity feature of the G1000-2 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 an AIS-P condition (see page 2-17), an LOP-P alarm (see page 2-80), a PDI-P alarm (see page 2-93), or an UNEQ-P alarm (see page 2-122) exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-2 Ethernet port is administratively disabled or it is reporting a CARLOSS (G Series) alarm (see page 2-33), the C2 byte in the SONET path overhead indicates a PDI-P alarm (see page 2-93) 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 condition to occur on the reporting port. In all cases the source problem is either in the SONET path being used by the G1000-2 port or the far- end G1000-2 port to which it is mapped.

Procedure: Clear the TPTFAIL (G-Series) Alarm

Step 1 An occurrence of TPTFAIL on a G1000-2 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-2 port that is mapped to the port. Clear any alarms being reported by the OC-N card on the G1000-2 circuit.

Step 2 If no alarms are reported by the OC-N card, or if a PDI-P alarm (see page 2-93) is reported, the problem might be on the far-end G1000-2 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.184 TRMT

- Major (MJ), Service Affecting (SA)

A Missing Transmitter (TRMT) alarm occurs when there is a transmit failure on the XTC-14 card because of an internal hardware failure. The card must be replaced.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-130 for the reporting XTC-14 card.

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

Step 2 If the alarm does not clear, call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).

2.6.185 TRMT-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Transmitter Missing (TRMT-MISS) alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its connector. Incorrect impedance is detected when a transmit cable is missing on the XTC-14 does not match the inserted card; for example, an SMB connector or a BNC connector connects to an XTC-14 card instead of an XTC-28-3 card.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

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

Procedure: Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the XTC-14 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.186 UNEQ-P

- Critical (CR), Service Affecting (SA)

An 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 might result from an incomplete circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Warning **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Deleting a circuit affects traffic.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note If you have created a new circuit but it has no signal, an UNEQ-P alarm is reported on the OC-N cards and an AIS-P condition (see page 2-17) is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Procedure: 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 dialog box.

Step 3 Click the **Select Affected Circuits** dialog box.

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 might 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). The node view 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 2-128.

b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

c. If any other columns contain VTT, repeat Step 6.

Step 7 If all ONS nodes in the ring appear in the CTC network view, verify or not whether there are incomplete circuits:

a. Click the **Circuits** tab.

b. Verify that INCOMPLETE is not listed in the State column of any circuits.

Step 8 If you find circuits listed as incomplete, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.

Complete the "Delete a Circuit" procedure on page 2-128.

Step 10 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 Procedure Guide*.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a. Click the **Circuits** tab.

b. Verify that the State 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 15327 Procedure Guide*.

Step 13 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the OC-N/DS-N cards.

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

Step 14 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.187 UNEQ-V

- Major (MJ), Service Affecting (SA)

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 **Invisible laser radiation might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-122.

Step 2 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.188 WKSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Working Switched To Protection (WKSWPR) condition occurs when a line experiences an LOS (OC-N) alarm (see page 2-84), an SF condition (see page 2-106), or an SD condition (see page 2-104).

Procedure: Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOF (OC-N) Alarm" procedure on page 2-80.

Step 2 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.189 WTR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Wait To Restore (WTR) condition occurs when a WKSWPR condition (see page 2-124) is raised the wait-to-restore time has not expired, meaning 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.

Note WTR is an informational condition. It does not require troubleshooting.

2.7 XTC Line Alarms

The XTC-28-3 card provides three choices of line types: ESF, D4, or Unframed. The choice of framing format determines the line alarms that the XTC-28-3 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 XTC-14 card reports the same STS alarms as the standard XTC-28-3 card does.

Table 2-8 DS3-12E Line Alarms

Alarm	UNFRAMED	D4	ESF
LOS	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF	No	Yes	Yes
IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk	Yes	Yes	Yes
Facility Lpbk	Yes	Yes	Yes
FE Lpbk	No	No	Yes
FE Common Equipment Failure	No	No	Yes
FE Equipment Failure-SA	No	No	Yes
FE LOS	No	No	Yes
FE LOF	No	No	Yes
FE AIS	No	No	Yes
FE IDLE	No	No	Yes
FE Equipment Failure-NSA	No	No	Yes

2.8 Common Procedures in Alarm Troubleshooting

This section gives common procedures that are frequently used when troubleshooting alarms. For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15327 Procedure Guide*.

Procedure: Identify a Ring ID or Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View** > **Go to Network View**.

Step 3 Click the **Provisioning** > **BLSR** tabs.

From the Ring ID column, record the Ring ID, 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.

Procedure: Change a Ring ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 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 ID in the Ring ID field.

Step 6 Click **Apply**.

Step 7 Click **Yes** at the Changing Ring ID dialog box.

Procedure: Change a Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View** > **Go to Network View**.

Step 3 Click the **Provisioning** > **BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, right-click the node on the ring map.

Step 6 Select **Set Node ID** from the shortcut menu.

Step 7 Enter the new ID in the field.

Step 8 Click **Apply**.

Procedure: Verify Node Visibility for Other Nodes

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 At the node view, click the **Provisioning** > **BLSR** tabs.

Step 3 Highlight a BLSR.

Step 4 Click **Ring Map**.

Step 5 Verify that each node in the ring appears on the ring map with a node ID and IP address.

Step 6 Click **Close**.

Procedure: Verify or Create Node DCC Terminations

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 At the node view, click the **Provisioning** > **SONET DCC** tabs.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

a. Click **Create**.

b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the **Shift** key.

c. In the Port State area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Procedure: Lock Out a BLSR Span

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Maintenance** > **BLSR** tabs.

Step 3 Click the BLSR row table cell under the West Switch column to reveal the drop-down menu.

Step 4 Choose **LOCKOUT SPAN** and click **Apply**.

Step 5 Click **OK** on the BLSR Operations dialog box.

Procedure: Clear a BLSR Span Lock Out

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 the **Maintenance** > **BLSR** tabs.

Step 3 Click the BLSR row table cell under the West Switch column to reveal the drop-down menu.

Step 4 Choose **CLEAR** and click **Apply**.

Step 5 Click **OK** on the BLSR Operations dialog box.

Procedure: Clear a UPSR Lock Out

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 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 4 In the Circuits on Span dialog box, choose **CLEAR** from the Perform UPSR Span Switching drop-down menu to remove a previously set switch command. Click **Apply**.

Step 5 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 6 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the switch state for all UPSR circuits is CLEAR.

Procedure: Switch Protection Group Traffic with an External Switching Command

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 Display the node view.

Step 3 In node view, click the **Maintenance** > **Protection** tabs.

Step 4 Double-click the protection group that contains the reporting card.

Step 5 Click the working/active card of the selected groups.

Step 6 Click **FORCE** and **Yes** in the Confirmation dialog box.

Procedure: Clear an External Switching Command

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 the **Maintenance** > **Protection** tabs.

Step 3 Double-click the protection group that contains the reporting card.

Step 4 Highlight either selected group.

Step 5 Click **CLEAR** and click **Yes** at the confirmation dialog box.

Procedure: Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

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

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** at the Delete Circuits dialog box.

Procedure: Clear a Loopback

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance** tab.

Step 4 In the Loopback Type column, determine if 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 menu and select **None**.

Step 6 In the State column, determine whether any port row shows a state other than INS.

Step 7 If a row shows a state other than INS, click in the column cell to display the drop-down menu and select **INS**.

Step 8 Click **Apply**.

Procedure: Reset the Active XTC Card in CTC

Caution Resetting the active XTC card can be service-affecting.

Note Before you reset the XTC, 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, go to Step 2.

Step 2 Identify the active XTC.

If you are looking at the physical ONS 15327, the ACT/STBY LED of the active XTC is green. The ACT/STBLY LED of the standby XTC is amber.

Step 3 Right-click the active XTC.

Step 4 Choose **Reset Card** from the shortcut menu.

Step 5 Click **Yes** at the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view. The reboot takes up to ten minutes.

Step 6 Verify that the reset is complete and error-free:

Double-click the node and ensure that the reset XTC is in standby mode and that the other XTC is active.

- If you are looking at the physical ONS 15327, the ACT/STBY LED of the active XTC is green. The ACT/STBLY LED of the standby XTC is amber.
- No new alarms appear in the **Alarms** window in CTC.
- If you are looking at the physical ONS 15327, the active XTC ACT/STBY LED is green, and the LED of the standby XTC is amber.

Procedure: Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, position the cursor over the high-speed slot reporting the alarm.

Step 3 Right-click and choose **RESET CARD** from the shortcut menu.

Step 4 Click **Yes** in the Are You Sure dialog box.

Procedure: Verify BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 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 what the system was originally provisioned for, 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**.

Procedure: Physically Replace a Card

Step 1 Open the card ejectors.

Step 2 Slide the card out of the slot.

Step 3 Open the ejectors on the replacement card.

Step 4 Slide the replacement card into the slot along the guide rails.

Step 5 Close the ejectors.

Procedure: Remove and Reinsert (Reseat) a Card

⚠ **Caution** Do not perform this action on the XTC card without the supervision and direction of the Cisco Technical Assistance Center (TAC). The Cisco TAC can be reached at (1-800-553-2447).

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Procedure: Remove and Reinsert Fan-Tray 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 15327.

Step 3 Close the retractable handles.

CHAPTER 3

Replace Hardware

This chapter provides procedures for replacing Cisco ONS 15327 hardware.

- 3.1 Replace the Fan-Tray Assembly, page 3-1—Complete this procedure to replace the fan-tray assembly.
- 3.2 Remove and Reinsert (Reseat) the Standby XTC, page 3-3—Complete this procedure as needed to reset the XTC by performing a card pull.
- 3.3 Inspect, Clean, and Replace the Reusable Air Filter, page 3-3—Complete this procedure to replace a reusable or disposable air filter.

3.1 Replace the Fan-Tray Assembly

You should not need to remove the fan-tray assembly unless a fan failure occurs and you must replace the fan-tray assembly. You cannot replace individual fans.

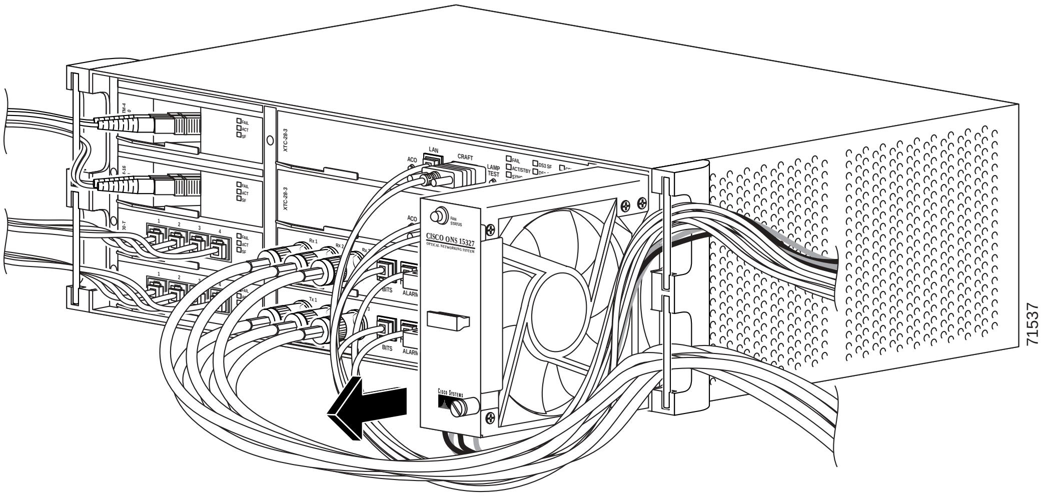
Step 1 Move any cables that are routed in front of the fan-tray assembly and air filter away so you can easily slide the filter out.

Step 2 Loosen the fastening screw on the failed fan-tray assembly.

Step 3 Grasp the fan tray handle and gently pull it one inch out of the slot and wait until the fans stop turning.

Step 4 When the fans have stopped turning, pull the fan-tray assembly completely out of the shelf assembly. (See Figure 3-1 on page 3-2.)

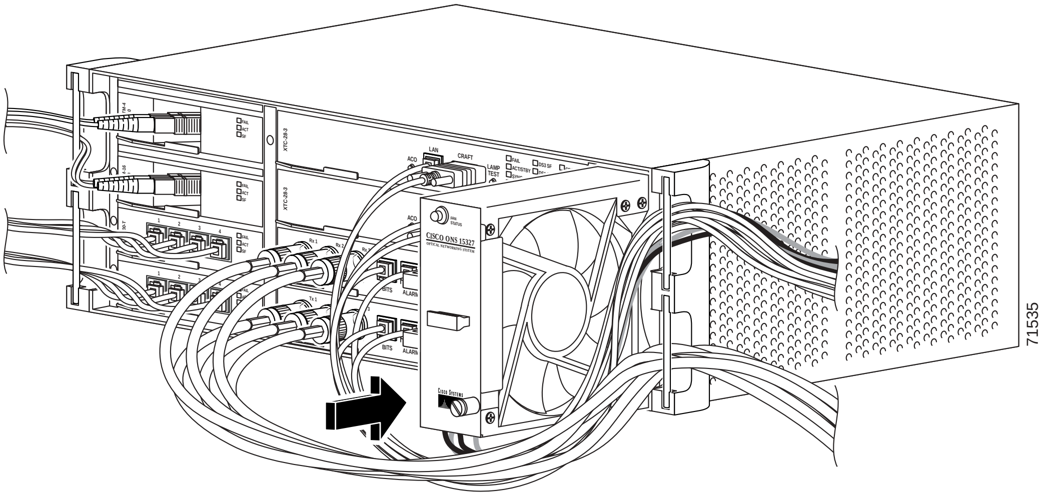
Figure 3-1 Removing the Fan-Tray Assembly



Step 5 Slide the new fan-tray assembly into the shelf until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the back panel (Figure 3-2).

Caution Do not force the fan-tray assembly into place while installing it. Forcing the fan-tray assembly into place can damage the connectors on the fan tray and/or the connectors on the shelf assembly.

Figure 3-2 Replacing the Fan-Tray Assembly



Step 6 Secure the fan-tray assembly into the slot using the attached fastening screw.

Step 7 Confirm that the FAN STATUS LED on the front of the fan-tray assembly is illuminated. This indicates that the fan is operating.

Note The FAN STATUS LED only illuminates when an XTC card is installed.

3.2 Remove and Reinsert (Reseat) the Standby XTC

Caution Do not perform this action without the supervision and direction of the Cisco Technical Assistance Center (TAC). The Cisco TAC can be reached at (1-800-553-2447).

Note To determine whether you have an active or standby XTC, position the cursor over the XTC card graphic to display the status.

Step 1 Ensure that the XTC you want to reset is in standby mode. On the XTC card, the ACT/STBY (Active/Standby) LED is amber when the XTC is in standby mode.

Step 2 When the XTC is in standby mode, unlatch both the top and bottom ejector levers on the XTC card.

Step 3 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 4 Wait 30 seconds. Reinsert the card and close the ejector levers.

Note The XTC will take several minutes to reboot and will display the amber standby LED after rebooting. Refer to the *Cisco ONS 15327 Procedure Guide* for more information about LED behavior during XTC reboots.

3.3 Inspect, Clean, and Replace the Reusable Air Filter

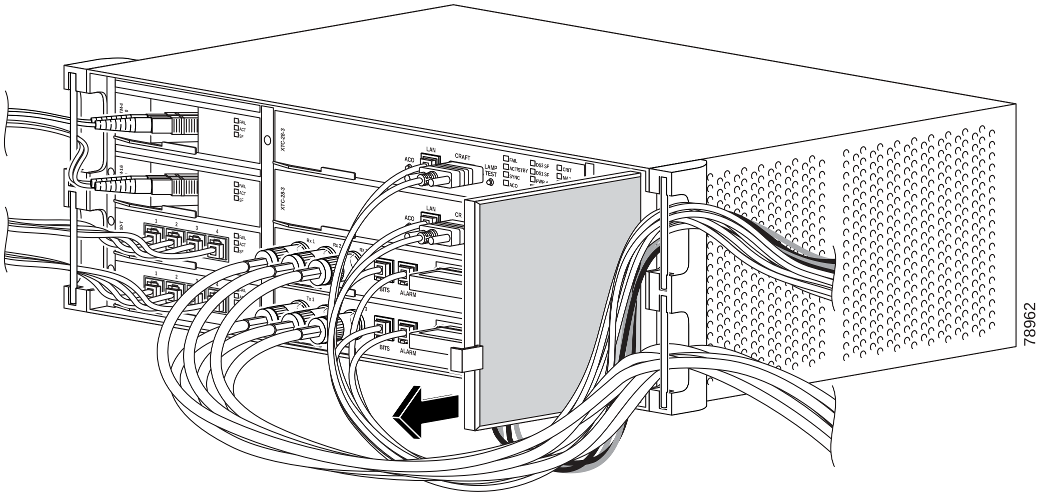
Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Note The Cisco ONS 15327 air filter should be removed and visually inspected approximately every 30 days, depending on the cleanliness of the operating environment. The filter is reusable and made of a gray open-cell polyurethane foam, specially coated to provide fire and fungi resistance. Figure 3-3 on page 3-4 illustrates the reusable fan-tray air filter. You do not need to remove the fan-tray assembly to remove the air filter.

Step 1 Move any cables that are routed in front of the fan-tray assembly and air filter so you can easily slide the filter out, as shown in Figure 3-3 on page 3-4.

Step 2 Grasp the metal tab at the edge of the filter and slide the filter out of the bracket while being careful not to dislodge any dust that may have collected on the filter.

Figure 3-3 Removing the Reusable Fan-Tray Air Filter



Step 3 Visually inspect the filter material for dirt and dust.

Step 4 If the reusable air filter contains a concentration of dirt and dust, vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a spare clean air filter (spare filters should be kept in stock).

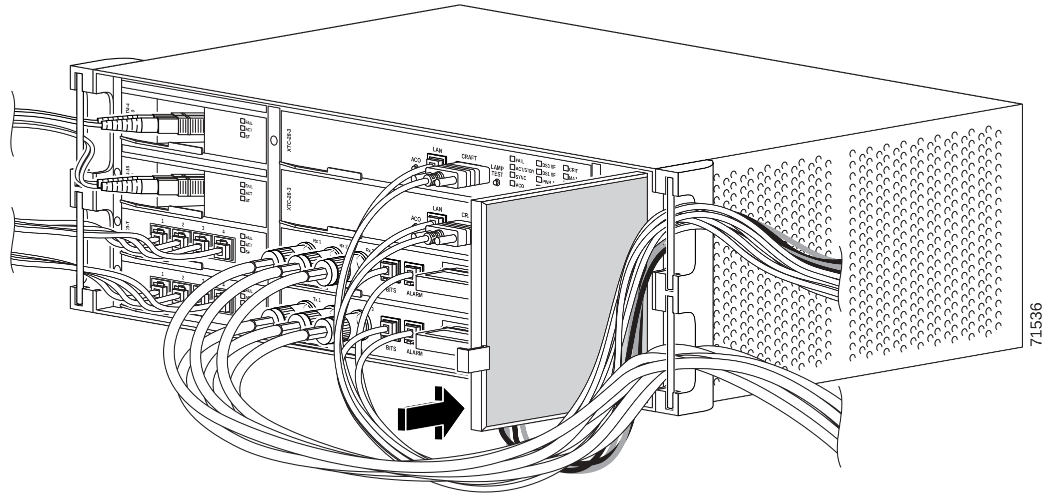
Step 5 Wash the dirty air filter under a faucet with a light detergent. After washing the air filter, allow it to completely air dry for at least eight hours before reusing.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Warning **Do not put a damp filter back in the ONS 15327.**

Step 6 Slide the clean air filter back into the shelf. (See Figure 3-4 on page 3-5.)

Figure 3-4 Replacing the Reusable Fan-Tray Air Filter



INDEX