CISCO SYSTEMS

# Cisco ONS 15454 Troubleshooting Guide

Product and Documentation Release 4.0
Last Updated: October 23, 2007

*Cisco ONS 15454 Troubleshooting Guide*

**CONTENTS**

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

**F I G U R E S**

**T A B L E S**

# About this Manual

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

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

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

# Revision History

| Date | Notes |
|------|-------|
| 04/06/2007 | Revision History Table added for the first time. |
| 08/31/2007 | Updated About this Manual chapter. |

# Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

## World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

# Documentation CD-ROM

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

# Ordering Documentation

You can order Cisco documentation in these ways:

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

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

# Documentation Feedback

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

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

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

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

We appreciate your comments.

# Obtaining Technical Assistance

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

# Cisco.com

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

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

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

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

http://www.cisco.com

# Technical Assistance Center

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

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

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

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

## Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

## Cisco TAC Escalation Center

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

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

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

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

# General Troubleshooting

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

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

- 1.2 Identify Points of Failure on a DS-N Circuit Path—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on a DS-N circuit.
- 1.3 Using the DS3XM-6 Card FEAC (Loopback) Functions—Describes the Far End Alarm and Control (FEAC) functions on the DS3XM-6 card.
- 1.4 Identify Points of Failure on an OC-N Circuit Path—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on an OC-N circuit.

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

- 1.5 Restoring the Database and Default Settings—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.6 PC Connectivity Troubleshooting—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- 1.7 CTC Operation Troubleshooting—Provides troubleshooting procedures for CTC login or operation problems.
- 1.8 Circuits and Timing—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.

- **1.9 Fiber and Cabling**—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- **1.10 Power and LED Tests**—Provides troubleshooting procedures for power supply and LED indicator problems.

# 1.1  Network Troubleshooting Tests

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

⚠ **Caution**    The facility or terminal loopback can be service-affecting. To protect traffic, apply a lockout or force switch to the target loopback port. For more information on these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

✎ **Note**    Facility loopback is not available for G1000-4 cards.

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

*Figure 1-1    Facility Loopback Process on a DS-N Card*
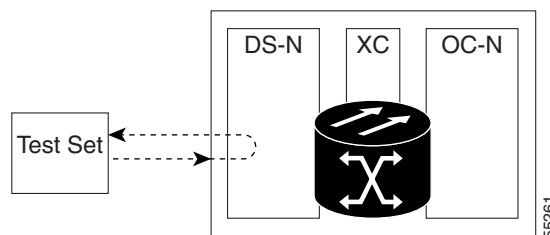


To test the LIU on an OC-N card, connect an optical test set to the OC-N port and perform a facility loopback or use a loopback or hairpin on a card that is farther along the circuit path. Figure 1-2 shows a facility loopback on an OC-N card.

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

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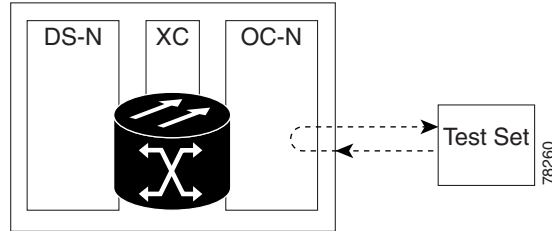


A terminal loopback tests a circuit path as it passes through the cross-connect card (XC, XCVT, or XC10G) and loops back from the card with the loopback. Figure 1-3 shows a terminal loopback on an OC-N card. The test-set traffic comes in on the DS-N card and goes through the cross-connect card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the DS-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the OC-N card.

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

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

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

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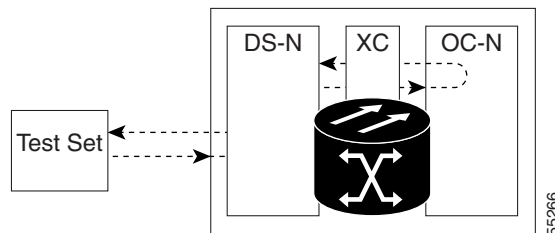


Figure 1-4 shows a terminal loopback on a DS-N card. The test-set traffic comes in on the OC-N card and goes through the cross-connect card to the DS-N card. The terminal loopback on the DS-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the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

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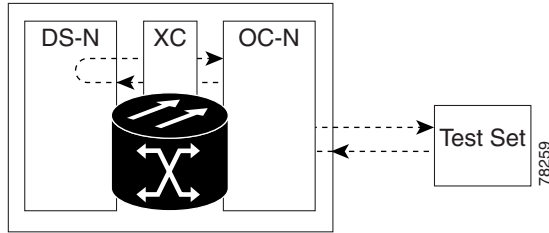


A hairpin circuit brings traffic in and out on a DS-N port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, thus preventing a drop of all traffic on the OC-N port. The hairpin allows you to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

*Figure 1-5    The Hairpin Circuit Process on a DS-N Card*
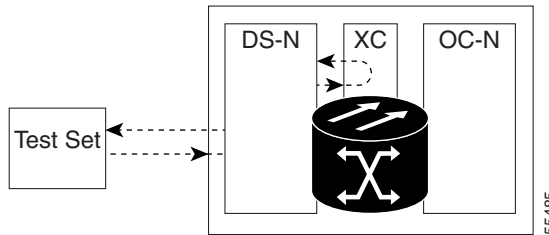


A cross-connect loopback tests a circuit path as it passes through the cross-connect card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel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

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    The Cross-connect Loopback Process on an OC-N Card*
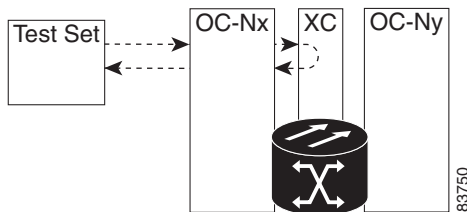
# 1.2  Identify Points of Failure on a DS-N Circuit Path

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

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

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

1. A facility loopback on the source node DS-N

2. A hairpin on the source node DS-N

3. A terminal loopback on the destination node DS-N

4. A hairpin on the destination node DS-N

5. A facility loopback on the destination DS-N

**Note**    All loopback tests require on-site personnel.

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

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

*Figure 1-7    A Facility Loopback on a Circuit Source DS-N Port*
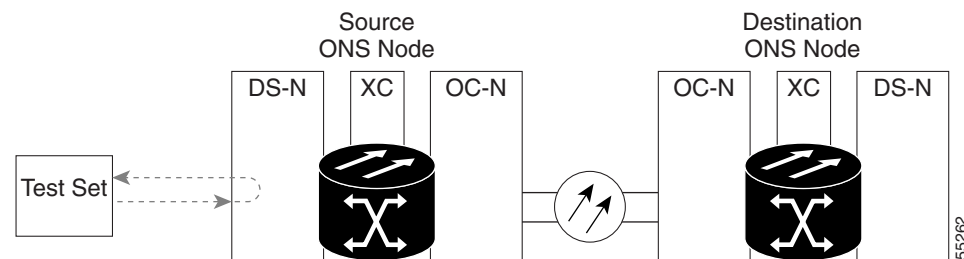


**Caution**    Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or force switch to the target loopback port. For more information on these operations, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure: Create the Facility Loopback on the Source DS-N Port

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

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

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

   **a.** In node view, double-click the card where you will perform 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** Complete the "Test the Facility Loopback Circuit" procedure on page 1-6.

## 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, 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.** Complete the "Perform a Hairpin on a Source Node Port" procedure on page 1-9.

**Step 4** If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

**Step 5** Complete the "Test the DS-N Cabling" procedure on page 1-7.

## Procedure: Test the DS-N Cabling

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

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

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

**Step 3**   If the test set indicates a good circuit, the problem was 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, 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.**   Complete the "Perform a Hairpin on a Source Node Port" procedure on page 1-9.

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

**Step 5**   Complete the "Test the DS-N Card" procedure on page 1-7.

## Procedure: Test the DS-N Card

**Step 1**   Replace the suspect card with a known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

⚠

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

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

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

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

   **b.**   Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-169 for details.

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

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

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

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

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

    **d.** Complete the "Perform a Hairpin on a Source Node Port" procedure on page 1-9.

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

**Step 5**    Complete the "Test the EIA" procedure on page 1-8.

## Procedure: Test the EIA

**Step 1**    Remove and reinstall the EIA to ensure a proper seating:

    **a.** Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

    **b.** Loosen the nine perimeter screws that hold the EIA panel in place.

    **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.

    **d.** Follow the installation procedure for the appropriate EIA. See the "3.6 Replace an Electrical Interface Assembly" section on page 3-17.

**Step 2**    Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA.

**Step 3**    If the test set indicates a good circuit, the problem was probably an improperly seated EIA.

    **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, 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 Step 8.

**Step 4**    If the test set indicates a faulty circuit, the problem is probably a defective EIA.

    **a.** Return the defective EIA to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC).

    **b.** Replace the faulty EIA. See the "3.6 Replace an Electrical Interface Assembly" section on page 3-17.

**Step 5**    Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.

**Step 6**    If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

**Step 7**    If the test set indicates a good circuit, the problem was probably the defective EIA.

    Clear the facility loopback:

- Click the **Maintenance > Loopback** tabs.
- Choose **None** from the Loopback Type column for the port being tested.
- Choose the appropriate state (IS, OOS, OOS_AINS) from the State column for the port being tested.

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

**Step 8**    Complete the "Perform a Hairpin on a Source Node Port" procedure on page 1-9.

## 1.2.2  Perform a Hairpin on a Source Node Port

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

*Figure 1-8    Hairpin on a Source Node Port*
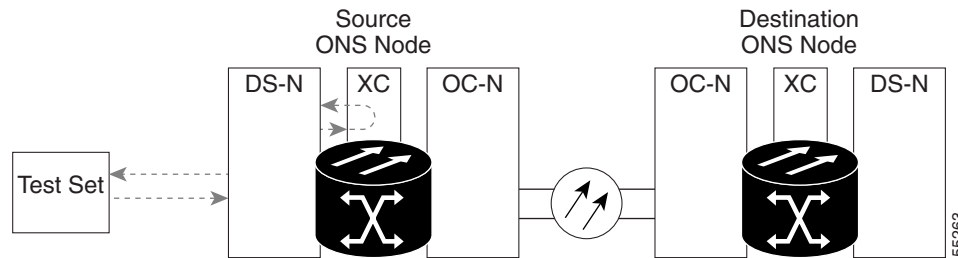


**Note**    The ONS 15454 does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

### Procedure: Create the Hairpin on the Source Node Port

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

- **a.** If you just completed the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. The Tx and Rx terminals connect to the same port.
- **c.** Adjust the test set accordingly.

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

- **a.** Click the **Circuits** tab and click the **Create** button.
- **b.** Give the circuit an easily identifiable name, such as Hairpin1.
- **c.** Set the Circuit **Type** and **Size** to the normal preferences.
- **d.** Uncheck the **Bidirectional** 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** Complete the

---

## Procedure: Test the Hairpin Circuit

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

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

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

> **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 box.
> - Confirm that the hairpin circuit is deleted form the Circuits tab list.
>
> **b.** Complete the

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

**Step 5** Complete the

---

## Procedure: Test the Standby Cross-Connect Card

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

> **a.** Determine the standby cross-connect card. On both the physical node and the Cisco Transport Controller (CTC) window, the ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
>
> **b.** Position the cursor over the standby cross-connect card.
>
> **c.** Right-click and choose **RESET CARD**.

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

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

> **a.** Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.
>
> **b.** In the node view, select the **Maintenance > Cross-Connect** tabs.

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

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

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

**Step 3**    Resend test traffic on the loopback circuit.

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

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

      **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 form the Circuits tab list.

      **b.** Complete the "Perform a Terminal Loopback on a Destination DS-N Port" procedure on page 1-12.

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

**Step 6**    To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-11.

## Procedure: Retest the Original Cross-Connect Card

**Step 1**    Initiate an external switching command (side switch) on the cross-connect cards to make the original cross-connect card the active card.

      **a.** Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

**Step 2**    Resend test traffic on the loopback circuit.

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

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

      **b.** Replace the defective cross-connect card. See Chapter 3, "Replace an In-Service Cross-Connect Card" 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 form the Circuits tab list.

**d.** Proceed to the Step 5.

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

Clear the hairpin circuit:

- 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 form the Circuits tab list.

**Step 5**    Complete the "Perform a Terminal Loopback on a Destination DS-N Port" procedure on page 1-12.

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

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

*Figure 1-9    Terminal Loopback on a Destination DS-N Port*
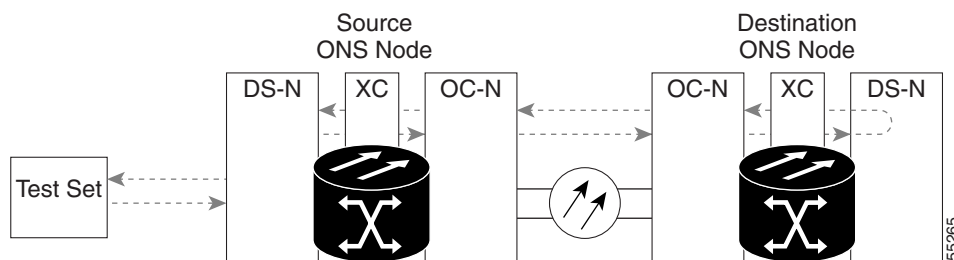


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

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

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

**a.** If you just completed the "Perform a Hairpin on a Source Node Port" procedure on page 1-9, leave the electrical test set hooked up to the DS-N port in the source node.

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

        **c.** Adjust the test set accordingly.

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

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

        **b.** Give the circuit an easily identifiable name, such as "DSNtoDSN."

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

        **d.** Leave the **Bidirectional** 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 DS-N port in the destination node) and click the **Finish** button.

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

> **Note**    It is normal for 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**    Complete the .

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

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

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

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

- **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, 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:
  - 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.** Complete the "Perform a Hairpin on a Destination Node" procedure on page 1-15.

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

**Step 5**  Complete the "Test the Destination DS-N Card" procedure on page 1-14.

## Procedure: Test the Destination DS-N Card

**Step 1**  Replace the suspect card with a known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

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

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

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

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

- **b.** Replace the defective DS-N card. See the "Physically Replace a Card" procedure on page 2-169 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, 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:

   - 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**    Complete the "Perform a Hairpin on a Destination Node" procedure on page 1-15.

# 1.2.4  Perform a Hairpin on a Destination Node

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

*Figure 1-10    Hairpin on a Destination Node*
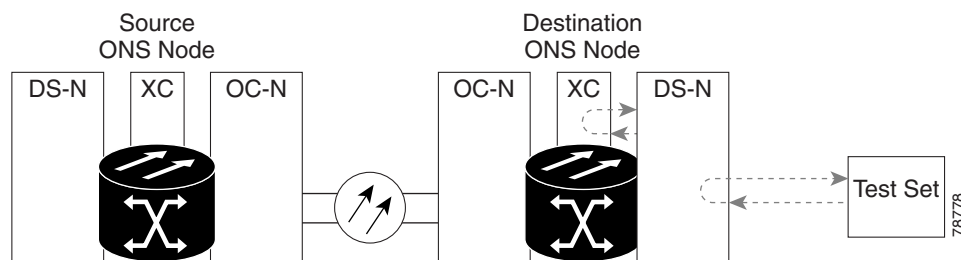


**Note**    The ONS 15454 does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

## Procedure: Create the Hairpin on the Destination Node

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

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

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

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

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

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

  d.  Uncheck the **Bidirectional** 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 in the Circuits tab list as a one-way circuit.

**Step 4** Complete 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 traffic on the loopback circuit.

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

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

    **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 form the Circuits tab list.

    **b.** Complete the "Perform a Facility Loopback on a Destination DS-N Port" procedure on page 1-18.

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

**Step 5** Complete the "Test the Standby Cross-Connect Card" procedure on page 1-16.

## Procedure: Test the Standby Cross-Connect Card

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

    **a.** Determine the standby cross-connect card. On both the physical node and the CTC window, the ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

⚠

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

    **a.**    Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

✎

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

**Step 3**    Resend test traffic on the loopback circuit.

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

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

    **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 form the Circuits tab list.

    **b.**    Complete the <span style="color:blue">"Perform a Facility Loopback on a Destination DS-N Port" procedure on page 1-18</span>.

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

**Step 6**    To confirm a defective original cross-connect card, complete the <span style="color:blue">"Retest the Original Cross-Connect Card" procedure on page 1-17</span>.

## Procedure: Retest the Original Cross-Connect Card

**Step 1**    Initiate an external switching command (side switch) on the cross-connect cards to make the original cross-connect card the active card.

    **a.**    Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

**Step 2**    Resend test traffic on the loopback circuit.

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

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

    **b.**    Replace the defective cross-connect card. See Chapter 3, "Replace an In-Service Cross-Connect Card".

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

- 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 cross-connect card might have had a temporary problem that was 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**    Complete the "Perform a Facility Loopback on a Destination DS-N Port" procedure on page 1-18.

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

The facility loopback test is performed on the node source port in the circuit, in this example, the destination DS-N port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination node cabling, DS-N card, LIU, or EIA is responsible for a faulty circuit. Figure 1-11 shows an example of a facility loopback on a destination DS-N port.

*Figure 1-11    Facility Loopback on a Destination DS-N Port*
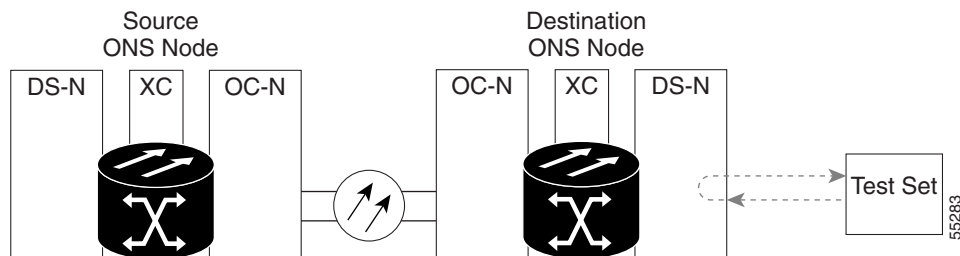


**Caution**    Performing a loopback on an in-service circuit is service-affecting.

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

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

   **a.**  If you just completed the "Perform a Hairpin on a Destination Node" procedure on page 1-15, leave the electrical test set hooked up to the DS-N port in the destination node.

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

   **c.**  Adjust the test set accordingly.

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

   **a.**  In node view, double-click the card where the loopback will be performed.

   **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**   Complete 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 traffic on the loopback circuit.

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

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

Clear the facility loopback:

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

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

**Step 4**   If the test set indicates a faulty circuit, the problem might be a faulty DS-N card, faulty cabling from the DS-N card to the DSx panel or the EIA, or a faulty EIA.

**Step 5**    Complete the "Test the DS-N Cabling" procedure on page 1-20.

## Procedure: Test the DS-N Cabling

**Step 1**    Replace the suspect cabling (the cables from the test set to the DSx panel or the EIA ports) with a cable that is known to be good.

- If a cable that is known to be good is not available, test the suspect cable with a test set. Remove the suspect cable from the DSx panel or the EIA and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or defective.

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

**Step 3**    If the test set indicates a good circuit, the problem was 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, OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

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

**Step 5**    Complete the "Test the DS-N Card" procedure on page 1-20.

## Procedure: Test the DS-N Card

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

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

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

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

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

    **b.**    Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-169 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, OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

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

**Step 5** Complete the "Test the EIA" procedure on page 1-21.

## Procedure: Test the EIA

**Step 1** Remove and reinstall the EIA to ensure a proper seating.

   **a.** Remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454, and pull it away from the shelf assembly.

   **b.** Loosen the nine perimeter screws that hold the EIA panel in place.

   **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.

   **d.** Follow the installation procedure for the appropriate EIA. See the "3.6 Replace an Electrical Interface Assembly" section on page 3-17 for details.

**Step 2** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA.

**Step 3** If the test set indicates a good circuit, the problem was probably an improperly seated EIA.

Clear the facility loopback:

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

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

**Step 4** If the test set indicates a faulty circuit, the problem is probably the defective EIA.

   **a.** Return the defective EIA to Cisco through the returned materials authorization (RMA) process. Contact the Cisco Technical Assistance Center (Cisco TAC) at 1-800-553-2447 or obtain a directory of toll-free Cisco TAC telephone numbers at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

   **b.** Replace the faulty EIA. See Chapter 3, "Replace an Electrical Interface Assembly" for details.

**Step 5** Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA.

**Step 6** If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

If the faulty circuit persists, contact the Cisco Technical Assistance Center (Cisco TAC).

**Step 7**    If the test set indicates a good circuit, the problem was probably the defective EIA.

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, OOS_AINS) from the State column for the port being tested.
- Click the **Apply** button.
- Click the **Yes** button in the Confirmation Dialog box.

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

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

The DS3XM-6 card supports Far End Alarm and Control (FEAC) functions that are not available on basic DS-3 cards. Click the Maintenance tab at the DS3XM-6 card view to reveal the two additional function columns. Figure 1-12 shows the DS3 subtab and the additional *Send Code* and *Inhibit FE Lbk* function columns.

*Figure 1-12   Accessing FEAC Functions on the DS3XM-6 Card*
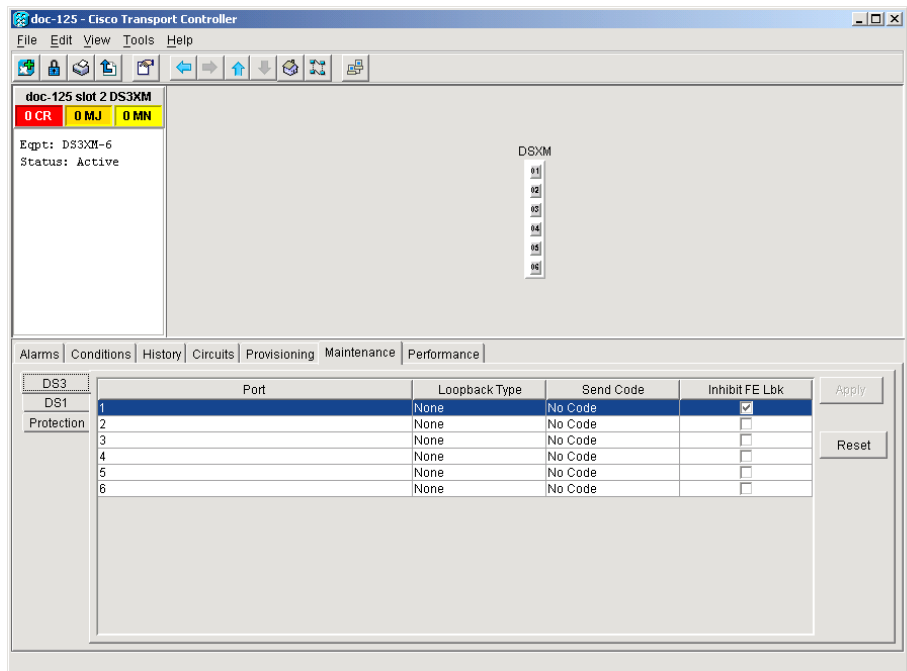


The far end in FEAC refers to the piece of equipment that is connected to the DS3XM-6 card and not the far end of a circuit. In Figure 1-13, if a DS3XM-6 (near-end) port is configured to send a Line Loop Code, the code will be sent to the connected test set, not the DS3XM-6 (far-end) port.

*Figure 1-13   Diagram of FEAC*
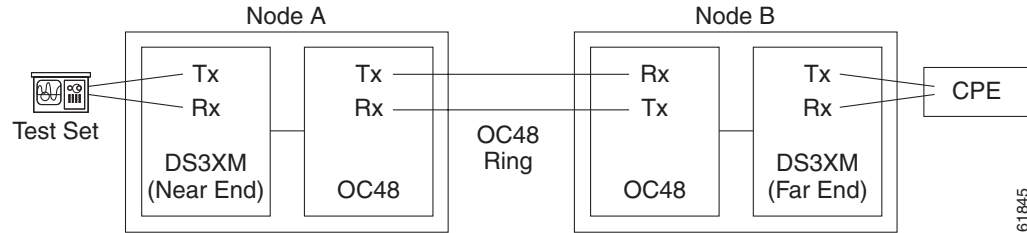


## 1.3.1  FEAC Send Code

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

## 1.3.2  FEAC Inhibit Loopback

The DS3XM-6 ports and transmuxed DS-1s initiate loopbacks when they receive FEAC Line Loop codes. If the Inhibit Loopback check box is checked for a DS-3 port, then that port will ignore any received FEAC Line Loop codes and will not loop back. The port can still be put into loopback manually using the Loopback Type column even if the Inhibit Loopback check box is selected. Only DS-3 ports can be configured to inhibit responses to FEAC loopback commands, individual DS-1 ports cannot inhibit their responses.

## 1.3.3  FEAC Alarms

The node raises a LPBKDS1FEAC-CMD or LPBKDS3FEAC-CMD condition for a DS-1 or DS-3 port if a FEAC loopback code is sent to the far end.

If the ONS 15454 port is in loopback from having received a loopback activate FEAC code, a LPBKDS1FEAC or LPBKDS3FEAC condition occurs. The condition will clear when a loopback deactivate FEAC command is received on that port.

A DS3E card will respond to, and can inhibit, received FEAC DS3 level loopback codes. A DS3E card cannot be configured to send FEAC codes.

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

Facility loopbacks, 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, bidirectional line switched ring (BLSR). Using a series of facility loopbacks and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of seven network test procedures apply to this example scenario:

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

1. A facility loopback on the source node OC-N port
2. A terminal loopback on the source node OC-N port
3. A cross-connect loopback on the source OC-N port
4. A facility loopback on the intermediate node OC-N port
5. A terminal loopback on the intermediate node OC-N port
6. A facility loopback on the destination node OC-N port
7. A terminal loopback on the destination node OC-N port

**Note**    All loopback tests require on-site personnel.

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

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the source node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Figure 1-14 shows an example of a facility loopback on a circuit source OC-N port.

*Figure 1-14    Facility Loopback on a Circuit Source OC-N Port*
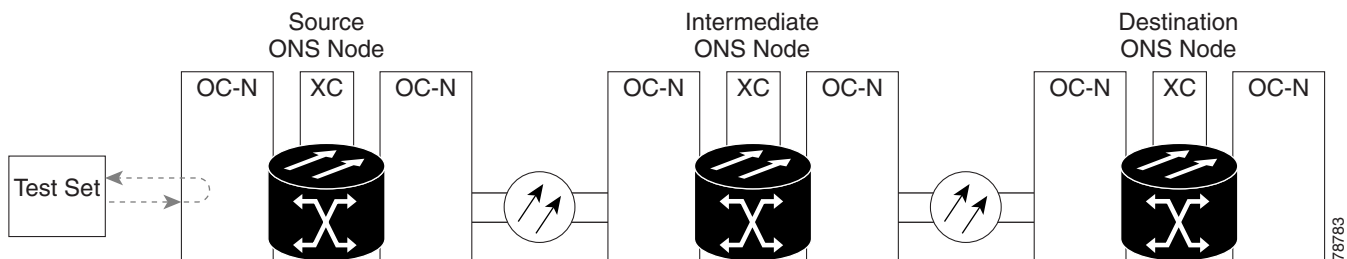


**Caution**    Performing a loopback on an in-service circuit is service-affecting.

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

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

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

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

    **a.**    In node view, double-click the card where you will perform 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**    Complete the "Test the Facility Loopback Circuit" procedure on page 1-25.

## 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, 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.**    Complete the "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-26.

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

**Step 5**    Complete the "Test the OC-N Card" procedure on page 1-25.

## Procedure: Test the OC-N Card

**Step 1**    Replace the suspect card with a known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

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

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

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

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

   **b.**    Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-169 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, 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**    Complete the "Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-26.

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

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the source node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then proceed with the terminal loopback test. Completing a successful terminal loopback to anode destination OC-N port verifies that the circuit is good up to the destination OC-N. Figure 1-15 shows an example of a terminal loopback on a destination OC-N port.

*Figure 1-15   Terminal Loopback on a Source-Node OC-N Port*
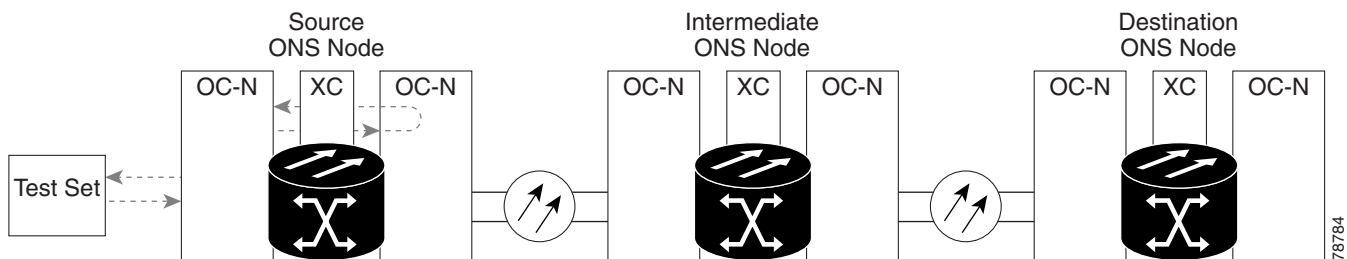


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

## 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 "1.4.1 Perform a Facility Loopback on a Source-Node OC-N Port" section on page 1-24, leave the optical test set hooked up to the OC-N port in the source node.

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

    **c.**    Adjust the test set accordingly.

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

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

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

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

    **d.**    Leave the **Bidirectional** 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 2-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**    Complete the "Test the Terminal Loopback Circuit" procedure on page 1-27.

## 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, 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.** Complete the "Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-32.

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

**Step 5** Complete the "Test the OC-N card" procedure on page 1-28.

## Procedure: Test the OC-N card

**Step 1** Replace the suspect card with a known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

⚠

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

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

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

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

    **b.** Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-169 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, 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**    Complete the "Create the XC Loopback on the Source OC-N Port" procedure on page 1-29.

## 1.4.3  Create the XC Loopback on the Source OC-N Port

The XC loopback test occurs on the cross-connect card in a network circuit. An XC loopback circuit uses the same port for both source and destination. Completing a successful XC loopback through the cross-connect card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-16 shows an example of an XC loopback on a source OC-N port.

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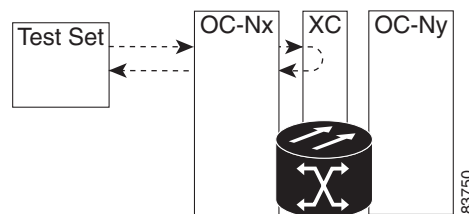


**Note**    An XC loopback breaks down an existing circuit path and creates a new cross-connect circuit (a hairpin), while the source of the original path is set to inject a line-side AIS-P condition. For instance, if you create an XC loopback from node A to node C through an intermediate node (B), the connection between A and B will be broken. Node C will be left with a one-way hairpin circuit back to A, and node A will inject an AIS-P signal. For more information about this condition, see the "2.6.3 AIS-P" section on page 2-22.

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

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

**a.** If you just completed the "1.4.2 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-26, leave the optical test set hooked up to the OC-N port in the source node.

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

**c.** Adjust the test set accordingly.

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

**a.**  In node view, 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** (Out of Service) or **OOS_MT** (Out of Service Maintenance) from the Status column for the port being tested.

**d.**  Click **Apply**.

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

**Step 3**  Use CTC to set up the XC 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.

**Step 4**  Complete the "Test the XC Loopback Circuit" procedure on page 1-30.

## Procedure: Test the XC 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 XC 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.**  Complete the "Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-32.

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

**Step 5**  Complete the "Test the Standby Cross-Connect Card" procedure on page 1-30.

## Procedure: Test the Standby Cross-Connect Card

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

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

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

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

**Step 2**    Initiate an external switching command (side switch) of the cross-connect cards before retesting the loopback circuit:

⚠

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

    **a.**   Determine the standby cross-connect card. The active cross-connect card displays a green ACT LED and the standby cross-connect card displays an amber SBY LED.

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

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

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

✎

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

**Step 3**    Resend test traffic on the loopback circuit.

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

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

    Clear the XC loopback circuit:

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

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

**Step 6**    To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-31.

## Procedure: Retest the Original Cross-Connect Card

**Step 1**    Initiate an external switching command (side switch) on the cross-connect cards to make the original cross-connect card the active card.

    **a.**   Determine the standby cross-connect card. The ACT/STBY LED of the standby cross-connect card is amber and the ACT/STBY LED of the active cross-connect card is green.

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

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

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

**Step 2**    Resend test traffic on the loopback circuit.

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

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

   **b.** Replace the defective cross-connect card. See the "Replace an In-Service Cross-Connect Card" procedure on page 3-1 for details.

   **c.** Clear the XC loopback circuit:

   - Click the **Circuits** tab.

   - Choose the XC loopback circuit being tested.

   - Click the **Delete** button.

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

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

Clear the XC loopback circuit:

   - Click the **Circuits** tab.

   - Choose the XC loopback circuit being tested.

   - Click the **Delete** button.

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

# 1.4.4  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 1-17 shows an example of a facility loopback on a intermediate node circuit source OC-N port.

*Figure 1-17   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 "1.4.2 Perform a Terminal Loopback on a Source-Node OC-N Port" section on page 1-26, leave the optical test set hooked up to the OC-N port in the source node.

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

   **c.**   Adjust the test set accordingly.

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

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

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

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

   **d.**   Leave the **Bidirectional** 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 intermediate node) and click the **Finish** button.

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

   **Note**   It is normal for 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 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**    Complete the "Test the Facility Loopback Circuit" procedure on page 1-34.

## 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, 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.**    Complete the "Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-35.

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

**Step 5**    Complete 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 known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

⚠️

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

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

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

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

      **b.** Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-169 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, 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**    Complete the "Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-35.

## 1.4.5  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 anode 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 an Intermediate-Node OC-N Port*
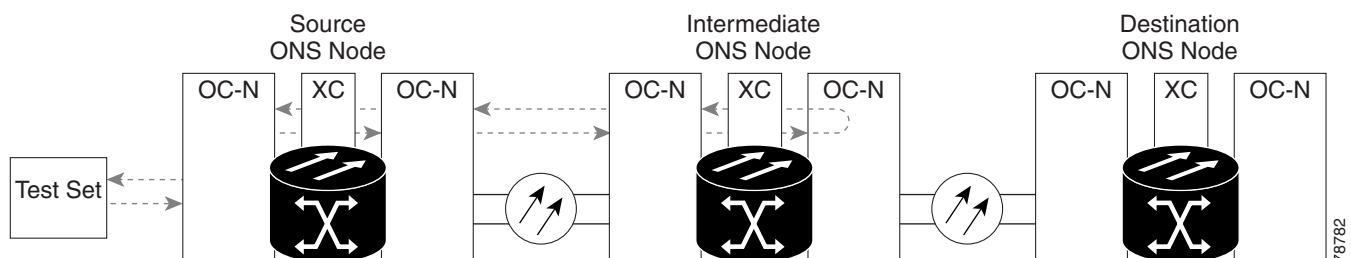


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

## 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 "1.4.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" section 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 transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.

    **c.** Adjust the test set accordingly.

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

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

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

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

    **d.** Leave the **Bidirectional** 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 intermediate node) and click the **Finish** button.

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

> ✎
>
> **Note**    It is normal for 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 dialog box.

**Step 5**  Complete the "Test the Terminal Loopback Circuit" procedure on page 1-37.

## 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, 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.**  Complete the "Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-38.

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

**Step 5**  Complete 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 known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

⚠

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

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

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

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

    **b.**  Replace the defective OC-N card. See the "Physically Replace a Card" procedure on page 2-169 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, 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** Complete the "Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-38.

## 1.4.6  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 1-19 shows an example of a facility loopback on a destination node circuit source OC-N port.

*Figure 1-19   Facility Loopback on a Destination Node OC-N Port*
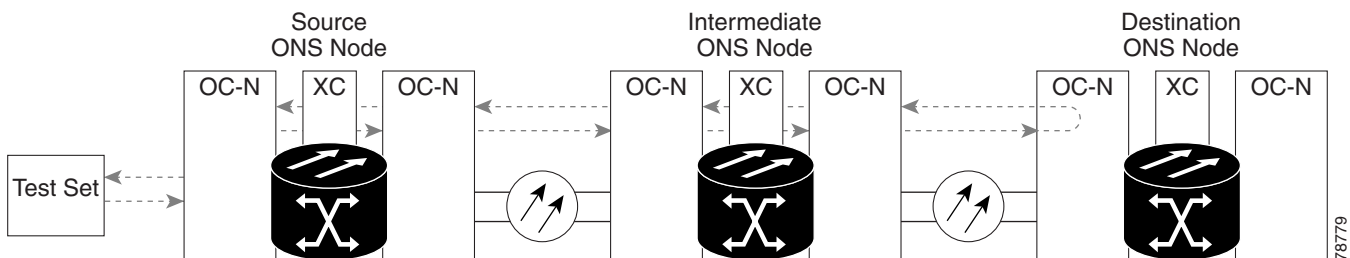


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

### 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 1-35, 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 transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.

    **c.**  Adjust the test set accordingly.

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

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

    **b.**  Give the circuit an easily identifiable name, such as "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 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 destination node) and click the **Finish** button.

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

> **Note**    It is normal for 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**    Complete the .

## 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, 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.**    Complete the "Perform a Terminal Loopback on a Destination Node OC-N Port" procedure on page 1-41.

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

**Step 5**    Complete 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 known-good card. See the "Physically Replace a Card" procedure on page 2-169 for details.

⚠️

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

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

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

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

    **b.**    Replace the faulty card. See the "Physically Replace a Card" procedure on page 2-169 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, 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**    Complete the .

## 1.4.7  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 1-20 shows an example of a terminal loopback on an intermediate node destination OC-N port.

*Figure 1-20   Terminal Loopback on a Destination Node OC-N Port*
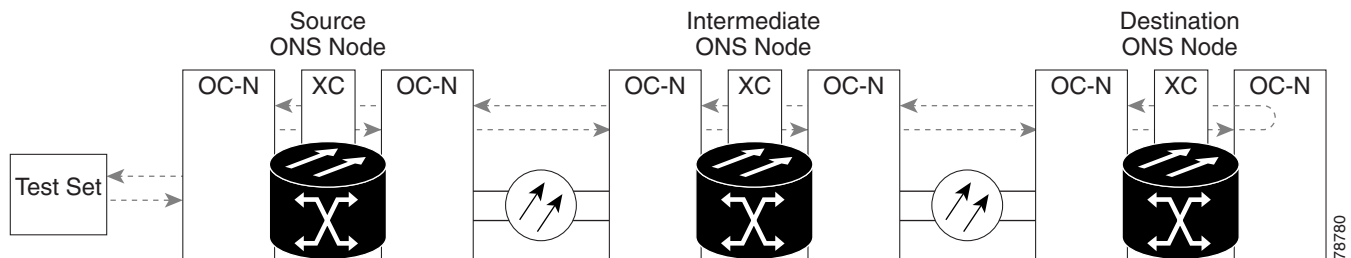


⚠
**Caution**    Performing a loopback on an in-service circuit is service-affecting.

## 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 1-38, leave the optical test set hooked up to the OC-N port in the source node.

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

   **c.** Adjust the test set accordingly.

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

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

   **b.** Give the circuit an easily identifiable name, such as "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 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 destination node) and click the **Finish** button.

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

✎

**Note** It is normal for 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 dialog box.

**Step 5** Complete the .

## 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, 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** Complete the .

## Procedure: Test the OC-N Card

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

⚠

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

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

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

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

    **b.** Replace the defective OC-N card. See the 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, 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.

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

# 1.5  Restoring the Database and Default Settings

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

## 1.5.1  Restore the Node Database

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

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

*Table 1-1    Restore the Node Database*

| Possible Problem | Solution |
|---|---|
| Incorrect or corrupted node database. | Perform a Restore the Database procedure. Refer to the "Restore the Database" procedure on page 1-44. |

## Procedure: Restore the Database

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

**Caution**   E1000-2 cards lose traffic for approximately 90 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning-tree reconvergence. The CARLOSS alarm appears and clears during this period.

**Caution**   If you are restoring the database on multiple nodes, wait until the TCC+/TCC2 reboot has completed on each node before proceeding to the next node.

**Step 1**   Log into the node where you will restore the database.

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

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

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

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

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

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

a. If there is a switch event (not caused by a line failure), clear the switch by choosing **CLEAR** from the 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 TCC+/TCC2 card.

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

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

## 1.5.2  Restore the Node to Factory Configuration

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

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

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

| Possible Problem | Solution |
|---|---|
| Failure of both TCC+/TCC2 cards in the node. | This procedure describes how to restore the node to factory configuration using the RE-INIT.jar JAVA file, which is referred to as the reinitialization tool in this documentation. Use this tool to upload the software package and/or restore the database after it has been backed up. You need the CD containing the latest software, the node's NE defaults, and the recovery tool. |
| Replacement of both TCC+/TCC2 cards at the same time. | Restore the node to factory configuration. Refer to the "Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" procedure on page 1-46 or the "Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" procedure on page 1-48. |

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

⚠ **Caution**    Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you only use the Search Path field. You 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 1-21 on page 1-47).

✎ **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 TCC+/TCC2 cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

**Step 1**    Insert the system software CD containing the reinit tool (Figure 1-21) 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 1-21).

*Figure 1-21   Reinitialization Tool in Windows*



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

**Step 6**   Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-21).

**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 1-22). Click **Yes**.

**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 TCC+/TCC2 successfully uploaded the database, not that the database restore was successful. The TCC+/TCC2 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 TCC+/TCC2 or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 13**   Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

*Figure 1-22   Confirm NE Restoration*
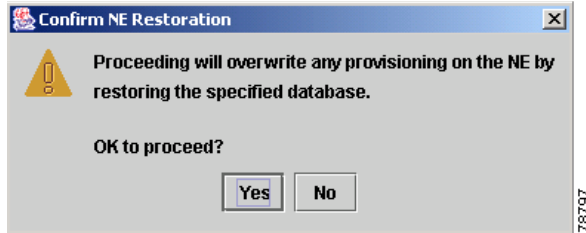


## Procedure: Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

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

**Note**   The TCC+/TCC2 cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

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

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

**Step 3**   If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinit tool (Figure 1-23). If you are working with a command line interface, run `java -jar RE-INIT.jar`.

*Figure 1-23   Reinitialization Tool in UNIX*
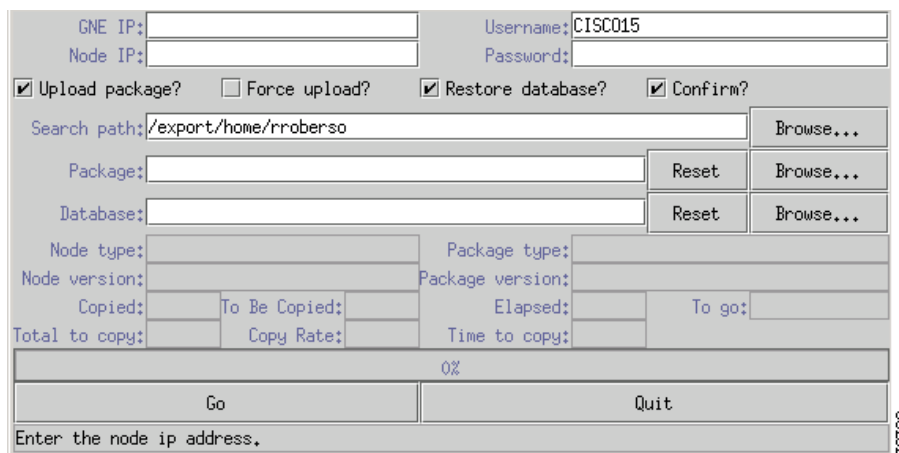


**Step 4**   If the node you are reinitializing is an end network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

**Step 5**   Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 1-23).

**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 . 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 TCC+/TCC2 successfully uploaded the database, not that the database restore was successful. The TCC+/TCC2 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 TCC+/TCC2 or on the hub or switch to which the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. Refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 12**    Manually set the node name and network configuration to site-specific values. Refer to the *Cisco ONS 15454 Procedure Guide* for information on setting the node name, IP address, mask and gateway, and IIOP port.

# 1.6  PC Connectivity Troubleshooting

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

## 1.6.1  Unable to Verify the IP Configuration of your PC

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

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

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

| Possible Problem | Solution |
|---|---|
| The IP address was typed incorrectly. | Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. See the "Verify the IP Configuration of Your PC" procedure on page 1-50. |
| 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 1-50. 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 will appear.

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

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

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

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

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

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

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

# 1.6.2  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 1-51 and the "Reconfigure the Browser" procedure on page 1-51. |

## 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 15454 software CD.

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

    **c.**  Double-click the **j2re-1_3_1_02-win** icon to run the JRE installation wizard.

    **d.**  Follow the JRE installation wizard steps.

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

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

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

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

**Step 7**    Click the **Apply** button.

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

## Procedure: Reconfigure the Browser

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

**Step 2**    If you are using Netscape Navigator:

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

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

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

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

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

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

        • For Windows 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 "1.7.3 Browser Stalls When Downloading CTC JAR Files From TCC+/TCC2" section on page 1-56.

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

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


# 1.6.3  Unable to Verify the NIC Connection on Your PC

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

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

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

| Possible Problem | Solution |
|---|---|
| The Cat-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 Cat-5 cable is damaged. | Ensure that the cable is in good condition. If in doubt, use a cable that is known to be good. Often, cabling is damaged due to pulling or bending |
| Incorrect type of Cat-5 cable is being used. | If connecting an ONS 15454 directly to your laptop/PC or a router, use a straight-through CAT-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover CAT-5 cable. |
| | For details on the types of Cat-5 cables, see the "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-79. |
| The NIC is improperly inserted or installed. | If you are using a PCMCIA based NIC, remove and re-insert the NIC to make sure the NIC is fully inserted. |
| | If the NIC is built into the laptop/PC, verify that the NIC is not faulty. |
| The NIC is faulty. | Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. |
| | If you have difficulty connecting a to the network (or any other node), then the NIC might be faulty and needs to be replaced. |

## 1.6.4  Verify PC Connection to the ONS 15454 (ping)

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

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

***Table 1-6    Verify PC connection to ONS 15454 (ping)***

| Possible Problem | Solution |
|---|---|
| A lost connection between the PC and the ONS 1554. | Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC+/TCC2 card. A ping command will work if the PC connects directly to the TCC+/TCC2 card or uses a LAN to access the TCC+/TCC2 card. |
| | See the "Ping the ONS 15454" procedure on page 1-53. |

### Procedure: Ping the ONS 15454

**Step 1**  Display the command prompt:

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

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

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

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

For example:

```
ping 192.1.0.2.
```

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

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

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

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

## 1.6.5  The IP Address of the Node is Unknown

**Symptom**  The IP address of the node is unknown and you are enable login.

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

*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 TCC+/TCC2 card in the shelf. Connect a PC directly to the remaining TCC+/TCC2 card and perform a hardware reset of the card. The TCC+/TCC2 card will transmit the IP address after the reset to enable you to capture the IP address for login.

See the "Retrieve Unknown Node IP Address" procedure on page 1-54. |

## Procedure: Retrieve Unknown Node IP Address

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

**Step 2**  Start the Sniffer application on your PC.

**Step 3**  Perform a hardware reset by pulling and reseating the active TCC+/TCC2 card.

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

# 1.7  CTC Operation Troubleshooting

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

## 1.7.1  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(s) of the symptom and the solution(s).

*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.

Reset Internet Explorer as the default browser so that CTC will associate the Help files to the correct browser.

See the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-55 to associate the CTC Help files to the correct browser. |

## Procedure: Reset Internet Explorer as the Default Browser for CTC

**Step 1**    Open the Internet Explorer browser.

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

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

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

**Step 5**    Click 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.

# 1.7.2  Unable to Change Node View to Network View

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

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

*Table 1-9    Browser Stalls When Downloading Files From TCC+/TCC2*

| Possible Problem | Solution |
|---|---|
| The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables. | Reset the system or user CTC_HEAP environment variable to increase the memory limits. See the "Reset the CTC_HEAP Environment Variable for Windows" procedure on page 1-55 or the "Reset the CTC_HEAP Environment Variable for Solaris" procedure on page 1-56 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 popup 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.

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
```

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

# 1.7.3  Browser Stalls When Downloading CTC JAR Files From TCC+/TCC2

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

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

*Table 1-10    Browser Stalls When Downloading jar File From TCC+/TCC2*

| Possible Problem | Solution |
|---|---|
| McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later. | Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scan" procedure on page 1-56. |

## 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.

## 1.7.4  CTC Does Not Launch

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

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

*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 1-57. |

### 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 the **Advanced** category and choose the **Cache** tab.

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

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

## 1.7.5  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(s) of the symptom and the solution(s).

*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 15454 to download a new set of jar files to your computer hard drive. See the "Delete the CTC Cache File Automatically" procedure on page 1-58 or the "Delete the CTC Cache File Manually" procedure on page 1-59. |

# Procedure: Delete the CTC Cache File Automatically

⚠

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

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

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

**Step 3**    Click the **Delete CTC Cache** button on the initial browser window to clear the CTC cache. Figure 1-24 shows the Delete CTC Cache window.

✎

**Note**    For CTC releases prior to 3.0, automatic deletion is unavailable. For CTC Cache file Manual deletion, see the "Delete the CTC Cache File Manually" procedure on page 1-59.

**Figure 1-24    Deleting the CTC Cache**
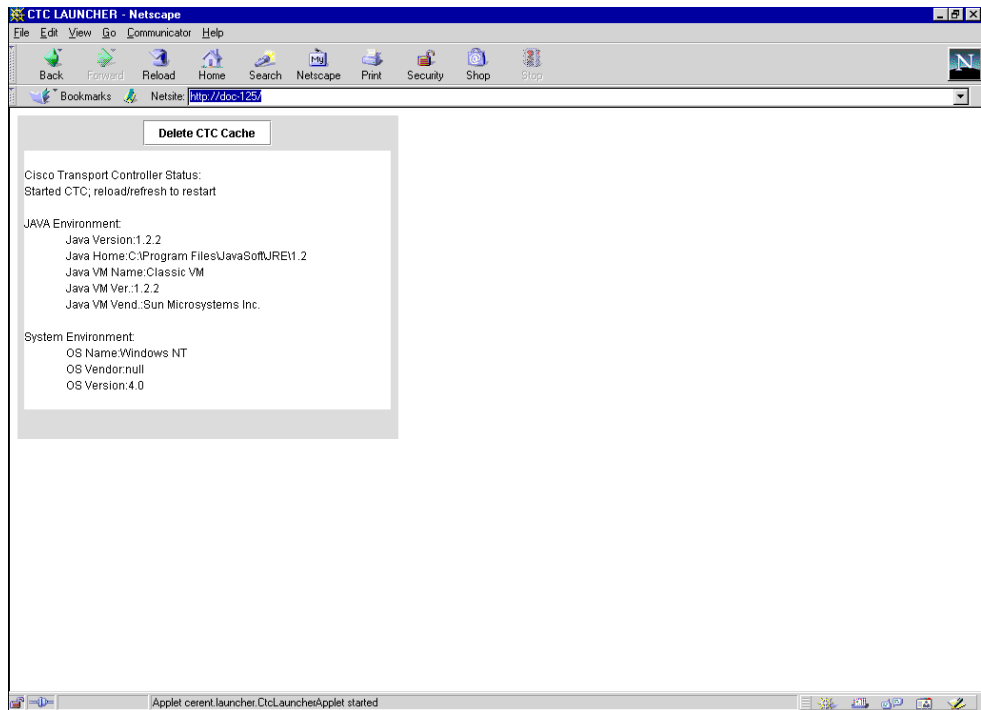
## Procedure: Delete the CTC Cache File Manually

⚠

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

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

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

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

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

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

## 1.7.6  Node Icon is Grey on CTC Network View

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

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

*Table 1-13    Node Icon is Grey on CTC Network View*

| Possible Problem | Solution |
|---|---|
| Different CTC releases not recognizing each other. | Correct the core version build as described in the "1.7.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-62. |
| A username/password mismatch. | Correct the username and password as described in the "1.7.10 Username or Password Do Not Match" section on page 1-63. |
| No IP connectivity between nodes. | Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.7.15 Ethernet Connections" section on page 1-65. |
| A lost DCC connection. | Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.54 EOC" section on page 2-57. |

## 1.7.7  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, or the java.policy file might be incomplete. | 1.  Verify that you have executed the javapolicyinstall.bat file on the ONS 15454 software CD. This file is installed when you run the CTC Setup Wizard (refer to the CTC installation information in the *Cisco ONS 15454 Procedure Guide* for instructions). <br><br> 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 1-60. |

## Procedure: Manually Edit the java.policy File

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

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

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

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

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

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

CTC should now start correctly.

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

# 1.7.8  Java Runtime Environment Incompatible

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

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

*Table 1-15    Java Runtime Environment Incompatible*

| Possible Problem | Solution |
|---|---|
| Do not have the compatible Java 2 JRE installed. | The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. |
| | The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-61. |
| | If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-16 shows JRE compatibility with ONS 15454 software releases. |

*Table 1-16    JRE Compatibility*

| ONS Software Release | JRE 1.2.2 Compatible | JRE 1.3 Compatible |
|---|---|---|
| ONS 15454 Release 2.2.1 and earlier | Yes | No |
| ONS 15454 Release 2.2.2 | Yes | Yes |
| ONS 15454 Release 3.0 | Yes | Yes |
| ONS 15454 Release 3.1 | Yes | Yes |
| ONS 15454 Release 3.2 | Yes | Yes |
| ONS 15454 Release 3.3 | Yes | Yes |
| ONS 15454 Release 3.4 | No | Yes |
| ONS 15454 Release 4.0 | No | Yes |

**Note**    Software R4.0 will notify you if an older version JRE is running on your PC or UNIX workstation.

## Procedure: Launch CTC to Correct the Core Version Build

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

**Step 2**    Start the browser.

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

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

![Note icon]

**Note**    After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

## 1.7.9  Different CTC Releases Do Not Recognize Each Other

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

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

*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 TCC+/TCC2 card are incompatible. | This occurs when the TCC+/TCC2 software is upgraded but the PC has not yet upgraded the compatible CTC jar file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version.<br><br>**Note**    Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node.<br><br>See the "Launch CTC to Correct the Core Version Build" procedure on page 1-62. |

## Procedure: Launch CTC to Correct the Core Version Build

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

**Step 2**   Start the browser.

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

**Step 4**   Log into CTC. The browser will download the jar file from CTC.

![Note icon]

**Note**    After Release 2.2.2, the single CMS.jar file evolved into core and element files. Core files are common to the ONS 15454, ONS 15454 SDH, and ONS 15327, while the element files are unique to the particular product. For example, the ONS 15327 Release 1.0 uses a 2.3 core build and a 1.0 element build. To display the CTC Core Version number, from the CTC menu bar click **Help > About CTC**. This lists the Core and Element builds discovered on the network.

# 1.7.10  Username or Password Do Not Match

**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 Do Not Match*

| Possible Problem | Solution |
|---|---|
| The username or password entered do not match the information stored in the TCC+/TCC2. | All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes.<br><br>For initial logon to the ONS 15454, type the CISCO15 user name in capital letters and click **Login** (no password is required). If you are using a CTC Software Release 2.2.2 or earlier and CISCO15  does not work, type cerent454 for the user name.<br><br>See the "Verify Correct Username and Password" procedure on page 1-63. |

## 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.

# 1.7.11  No IP Connectivity Exists Between Nodes

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

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

*Table 1-19    No IP Connectivity Exists Between Nodes*

| Possible Problem | Solution |
|---|---|
| A lost Ethernet connection. | Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.7.15 Ethernet Connections" section on page 1-65. |

## 1.7.12  DCC Connection Lost

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

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

*Table 1-20   DCC Connection Lost*

| Possible Problem | Solution |
|---|---|
| A lost DCC connection. | Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.6.54 EOC" section on page 2-57. |

## 1.7.13  "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 describes the potential cause(s) of the symptom and the solution(s).

*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 will get the "Path in Use" error. |
| | Cancel the circuit creation and start over, or click the **Back** button until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again. |

# 1.7.14 Calculate and Design IP Subnets

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

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

# 1.7.15 Ethernet Connections

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

Table 1-23 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-23    Calculate and Design IP Subnets*

| Possible Problem | Solution |
|---|---|
| Improperly seated connections. | You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-25 when consulting the steps in the "Verify Ethernet Connections" procedure on page 1-66. |
| Incorrect connections. | |

*Figure 1-25    Ethernet Connectivity Reference*



Device "A"
192.168.1.25
255.255.255.0
VLAN #1 Member

Device "B"
192.168.1.75
255.255.255.0
VLAN #1 Member

Virtual
LAN # 1

ONS Node #1
Port #1 VLAN #1
Port #3 VLAN #1

ONS Node #2
Port #1 VLAN #1
Port #2 VLAN #1

Device "C"
192.168.1.50
255.255.255.0
VLAN #1 Member

Device "D"
192.168.1.100
255.255.255.0
VLAN #1 Member

32167
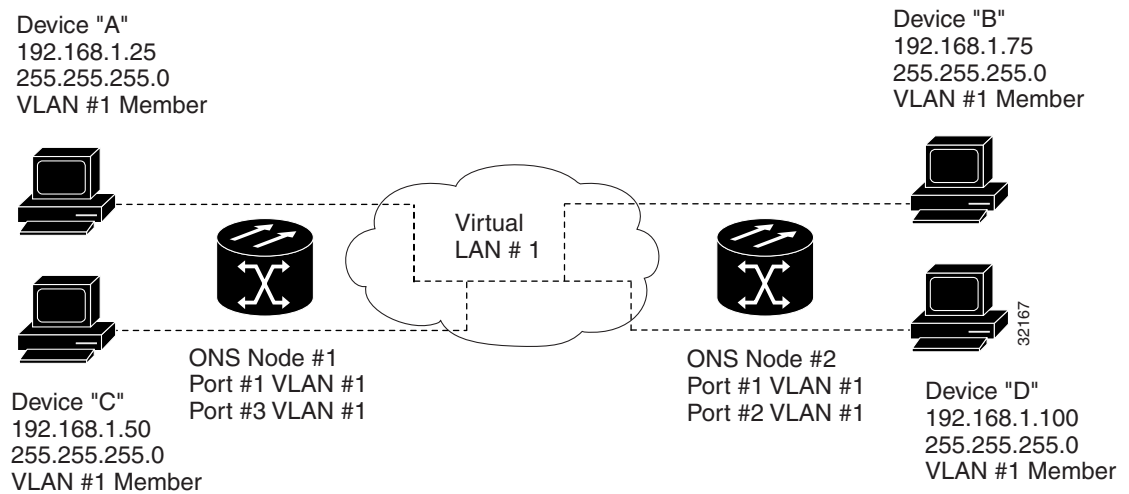
## Procedure: Verify Ethernet Connections

**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 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.

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

    **a.**    Verify physical connectivity between the ONS 15454s and the attached device.

    **b.**    Verify that the ports are enabled on the Ethernet cards.

    **c.**    Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

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

    **e.**    It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Run the procedure in the "1.10.3 Lamp Test for Card LEDs" section on page 1-86.

**Step 7**    Verify connectivity between device A and device C by pinging between these locally attached devices (see the "1.6.4 Verify PC Connection to the ONS 15454 (ping)" section on page 1-53). 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 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

# 1.7.16  VLAN Cannot Connect to Network Device from Untag Port

**Symptom**  Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-26). 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 1-26   A VLAN with Ethernet ports at Tagged and Untag*
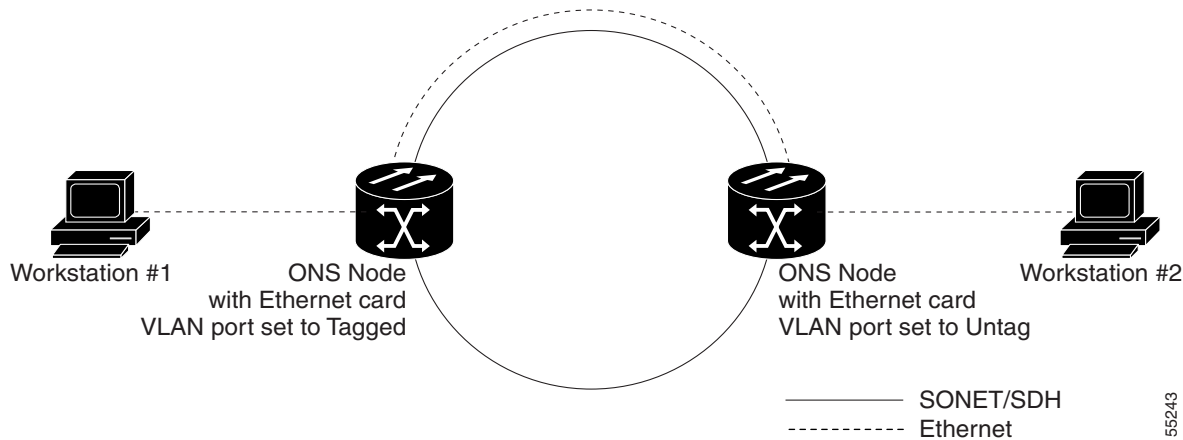


Table 1-24 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-24   Verify VLAN Connection to Network Device from Untag Port*

| Possible Problem | Solution |
|---|---|
| The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet. | The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance. |
| 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 1-27).
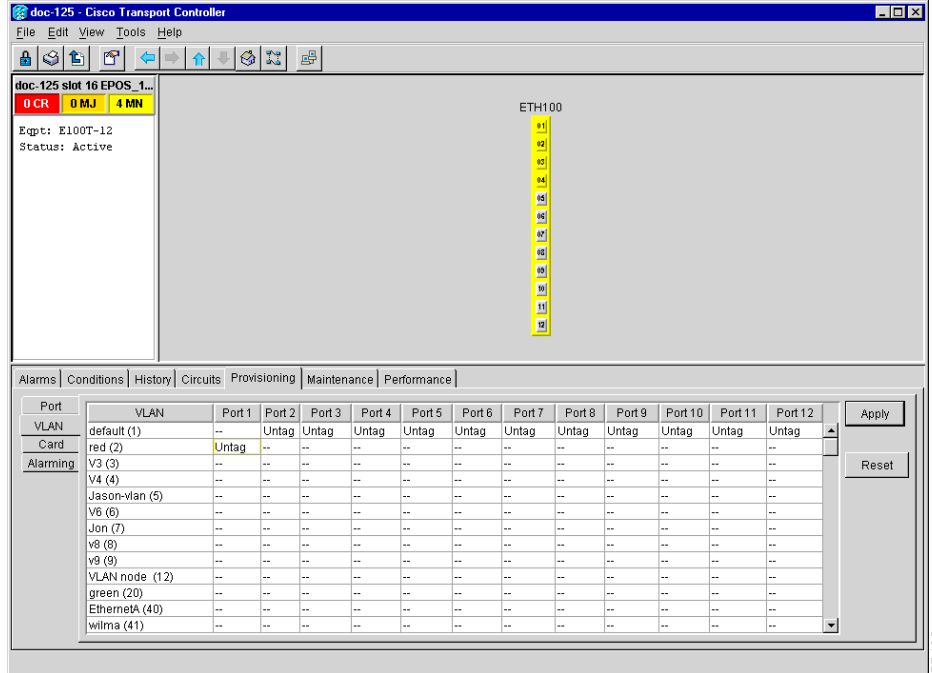
**Step 3**   If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.

**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**.

## 1.7.17  Cross-Connect Card Oscillator Fails

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

- SWMTXMOD against one or both cross-connect cards
- SD-L against near-end or far-end line cards
- AIS-L against far-end line cards
- RFI-L against near-end line cards

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

*Table 1-25    Cross-Connect Card Oscillator Fails*

| Possible Problem | Solution |
|---|---|
| The XC, XCVT, or XC10G card has oscillator failure. | 1.  If the Slot 8 cross-connect card is active, see the "Procedure:  Resolve the XC Oscillator Failure When Slot 8 XC Card is Active" section on page 1-69. |
|  | 2.  If the Slot 10 cross-connect card is active, see the "Procedure:  Resolve the XC Oscillator Failure When Slot 10 XC Card is Active" section on page 1-69. |

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

**Step 1**  If the CTNEQPT-PBPROT condition is reported against all I/O cards in the node and the Slot 8 cross-connect card is active, right-click the Slot 10 cross-connect card.

**Step 2**  Choose **Reset Card,** then click **OK**. (Slot 8 remains active and Slot 10 remains standby.)

**Step 3**  If the alarm remains, reseat the Slot 10 card.

**Step 4**  If CTNEQPT-PBPROT does not clear, replace the Slot 10 cross-connect card with a spare card.

**Step 5**  If CTNEQPT-PBPROT does not clear, replace the spare card placed in Slot 10 with the original cross-connect card.

**Step 6**  Right-click the Slot 8 card and choose **Reset Card**.

**Step 7**  Click **OK** to activate the Slot 10 card and place the Slot 8 card in standby.

**Step 8**  If you then see the CTNEQPT-PBWORK condition raised against all I/O cards in the node, verify that CTNEQPT-PBPROT has cleared on all I/O cards. Seeing CTNEQPT-PBWORK on the cards indicates that Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. Otherwise, go toStep 9.

    **a.**  Replace the Slot 8 cross-connect card with a spare card. (Slot 8 remains standby.)

    **b.**  Reseat the Slot 10 cross-connect card to activate the Slot 8 card and make Slot 10 standby.

    **c.**  Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

**Step 9**  If you see CTNEQPT-PBPROT reported against all I/O cards in the node, this indicates that the Slot 10 card has a bad oscillator. If so, complete the following steps:

    **a.**  Replace the Slot 10 cross-connect card with a spare card. (The Slot 8 card is now active.)

    **b.**  Reseat the Slot 8 cross-connect card to make Slot 10 active.

    **c.**  Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

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

**Step 1**  If the CTNEQPT-PBWORK condition is reported against all I/O cards in the node and the Slot 10 card is active, right-click the Slot 8 cross-connect card.

**Step 2**  Choose **Reset Card** and click **OK**. (Slot 10 remains active and Slot 8 remains standby.)

**Step 3**  If the CTNEQPT-PBWORK condition does not clear, reseat the Slot 8 cross-connect card.

**Step 4**   If the condition does not clear, replace the Slot 8 cross-connect card with an identical, spare card.

**Step 5**   If the condition does not clear, replace the spare card placed in Slot 8 with the original cross-connect card.

**Step 6**   Right-click the Slot 10 cross-connect card.

**Step 7**   Choose **Reset Card** and click **OK**. The Slot 8 cross-connect card becomes active and Slot 10 becomes standby.

**Step 8**   If you have switched the Slot 8 card to active and continue to see CTNEQPT-PBWORK reported against all I/O cards in the node, this indicates the Slot 8 card has a bad oscillator. If this is indicated, complete the following substeps. If not, go to Step 9.

   **a.**   Replace the Slot 8 cross-connect card with a spare card. (The Slot 10 card is made active.)

   **b.**   Reseat the Slot 10 cross-connect card to make Slot 8 active.

   **c.**   Verify that the CTNEQPT-PBWORK condition has cleared on all I/O cards.

**Step 9**   If you then see the CTNEQPT-PBPROT condition raised against all I/O cards, verify that CTNEQPT-PBWORK has cleared on the I/O cards. This indicates that Slot 10 has a bad oscillator. If so, complete the following substeps:

   **a.**   Replace the Slot 10 cross-connect card with a spare card. (Slot 10 remains standby.)

   **b.**   Reseat the Slot 8 cross-connect card to activate the Slot 10 card and make Slot 8 standby.

   **c.**   Verify that the CTNEQPT-PBPROT condition has cleared on all I/O cards.

# 1.8  Circuits and Timing

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

## 1.8.1  Circuit Transitions to Partial State

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

- OOS_PARTIAL   At least one of the connections in the circuit is in OOS state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.

- OOS_MT_PARTIAL   At least one connection in the circuit is in OOS_MT state and at least one other connection in the circuit is in IS, OOS_MT, or OOS_AINS state.

- OOS_AINS_PARTIAL   At least one connection in the circuit is in the OOS_AINS state and at least one other connection in the circuit is in IS or OOS_AINS state.

Table 1-26 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-26    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 1-71. |
| | 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 15454 Software Upgrade Guide* for software upgrade procedures. |
| | **Note**    If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by only using the circuit state(s) supported in the earlier software version. |
| During an automatic transition, some path-level defects and/or alarms were detected on the circuit. | Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-71. |
| | Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to clear alarms and change circuit configuration settings. |
| One end of the circuit is not properly terminated. | Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state. |

## 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.

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

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

Table 1-27 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-27    Calculate and Design IP Subnets*

| Possible Problem | Solution |
|---|---|
| The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service. | An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 VT circuits that are not carrying traffic and on stranded bandwidth. Perform the "Clear AIS-V on DS3XM-6 Unused VT Circuits" procedure on page 1-72. |

## Procedure: Clear AIS-V on DS3XM-6 Unused VT Circuits

**Step 1**    Determine the affected port.

**Step 2**    Record the node ID, slot number, port number, or VT number.

**Step 3**    Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

**Step 4**    Uncheck the bidirectional check box in the circuit creation window.

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

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

**Step 7**    Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

**Step 8**    From the Loopback Type list, choose **Facility (line)** and click **Apply**.

**Step 9**    Click **Circuits**.

**Step 10**   Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**.

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

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

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

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

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

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

# 1.8.3  Circuit Creation Error with VT1.5 Circuit

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

Table 1-28 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-28    Circuit Creation Error with VT1.5 Circuit*

| Possible Problem | Solution |
|---|---|
| You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message. | The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a path protection configuration or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Manual* for more information. |

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

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

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

*Table 1-29    Unable to Create Circuit from DS-3 Card to DS3XM-6 Card*

| Possible Problem | Solution |
|---|---|
| A DS-3 card and a DS3XM-6 card have different functions. | A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. Thus you can create a circuit from a DS3XM-6 card to a DS-1 card, but not from a DS3XM-6 card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 has a VT payload with a C2 hex value of 02. |
| | **Note**    You can find instructions for creating circuits in the *Cisco ONS 15454 Procedure Guide*. |

## 1.8.5  DS3 Card Does Not Report AIS-P From External Equipment

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

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

*Table 1-30    DS3 Card Does Not Report AIS-P From External Equipment*

| Possible Problem | Solution |
|---|---|
| The card is functioning as designed. | This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. |
| | DS3-12/DS3N-12/DS3-12E/DS3N-12E cards have DS3 header monitoring functionality, which allows you to view performance monitoring (PM) on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information on the PM capabilities of the DS3-12/DS3N-12/DS3-12E/DS3N-12E cards, refer to the *Cisco ONS 15454 Procedure Guide*. |

## 1.8.6  OC-3 and DCC Limitations

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

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

*Table 1-31    OC-3 and DCC Limitations*

| Possible Problem | Solution |
|---|---|
| OC-3 and DCC have limitations for the ONS 15454. | For an explanation of OC-3 and DCC limitations, refer to the DCC Tunnels section of the *Cisco ONS 15454 Procedure Guide*. |

## 1.8.7  ONS 15454 Switches Timing Reference

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

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

*Table 1-32    ONS 15454 Switches Timing Reference*

| Possible Problem | Solution |
|---|---|
| The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source. | The ONS 15454 internal clock operates at a Stratum 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of ± 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x $10^{-7}$/day, including temperature. |
| The optical or BITS input is not functioning. | |
| Sync Status Messaging (SSM) message is set to Don't Use for Sync (DUS). | |
| SSM indicates a Stratum 3 or lower clock quality. | ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source. |
| The input frequency is off by more than 15 ppm. | |
| The input clock wanders and has more than three slips in 30 seconds. | |
| A bad timing reference existed for at least two minutes. | |

## 1.8.8  Holdover Synchronization Alarm

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

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

*Table 1-33    Holdover Synchronization Alarm*

| Possible Problem | Solution |
|---|---|
| The last reference input has failed. | The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the "2.6.106 HLDOVRSYNC" section on page 2-87 for a detailed description of this alarm. |
| | **Note**    The ONS 15454 supports holdover timing per Telcordia standard GR-4436 when provisioned for external (BITS) timing. |

## 1.8.9  Free-Running Synchronization Mode

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

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

*Table 1-34    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 "2.6.96 FRNGSYNC" section on page 2-82 for a detailed description of this alarm. |

## 1.8.10  Daisy-Chained BITS Not Functioning

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

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

*Table 1-35    Daisy-Chained BITS Not Functioning*

| Possible Problem | Solution |
|---|---|
| Daisy-chaining BITS is not supported on the ONS 15454. | Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454. |

## 1.8.11  Blinking STAT LED after Installing a Card

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

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

*Table 1-36   Blinking STAT LED on installed card*

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

# 1.9  Fiber and Cabling

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

## 1.9.1  Bit Errors Appear for a Traffic Card

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

Table 1-37 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-37   Bit Errors Appear for a Line Card*

| Possible Problem | Solution |
|---|---|
| Faulty cabling or low optical-line levels. | Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using the "1.9.2 Faulty Fiber-Optic Connections" section on page 1-77. |

## 1.9.2 Faulty Fiber-Optic Connections

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

Table 1-38 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-38    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 1-77. |
| Faulty CAT-5 cables. | Faulty CAT-5 cables can be the source of SONET alarms and signal errors. See the "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-79. |
| Faulty gigabit interface connectors. | Faulty gigabit interface converters can be the source of SONET alarms and signal errors. See the "1.9.2.2 Replace Faulty GBIC or SFP Connectors" section on page 1-81. |

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

## Procedure: Verify Fiber-Optic Connections

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

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

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

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

**a.**  Remove the receive (Rx) end of the suspect fiber.

**b.**  Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.

**c.**  Determine the power level of fiber with the fiber-optic power meter.

**d.**  Verify the power meter is set to the appropriate wavelength for the 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 "1.9.3 Optical Card Transmit and Receive Levels" section on page 1-84.

**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 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

    **b.**   Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

    **c.**   Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.

       IR cards transmit a lower output power than LR cards.

    **d.**   Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-N card.

⚠️

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

    **e.**   If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

      • Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.

      • Excessive number or fiber connectors; connectors take approximately 0.5 dB each.

      • Excessive number of fiber splices; splices take approximately 0.5 dB each.

✎

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

⚠️

**Caution**   The fibers must be removed from the OC-N connectors before performing an OTDR test. Failure to disconnect the OC-N cards could result in permanent damage to the optical card.

**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 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

    **c.**   Retest the fiber power level.

    **d.**   If the replacement fiber still shows no power, replace the optical card.

⚠️

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

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

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

Receiver overloads occur when maximum receiver power is exceeded.

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

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

## 1.9.2.1  Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-28 shows the layout of an RJ-45 connector. Figure 1-29 and Table 1-39 shows a LAN cable layout and pinouts.

***Figure 1-28   RJ-45 Pin Numbers***



End view of RJ-45 plug                    Looking into an RJ-45 jack
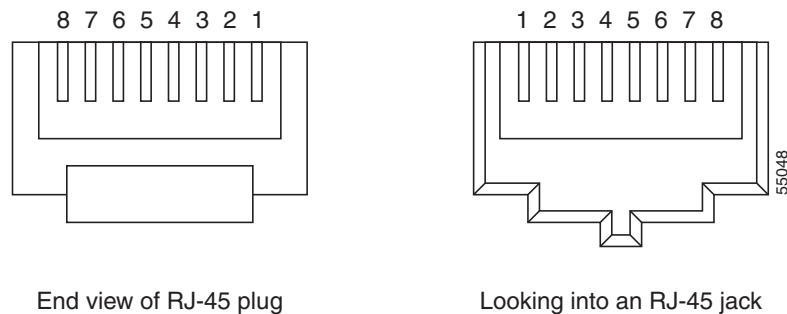
*Figure 1-29   LAN Cable Layout*
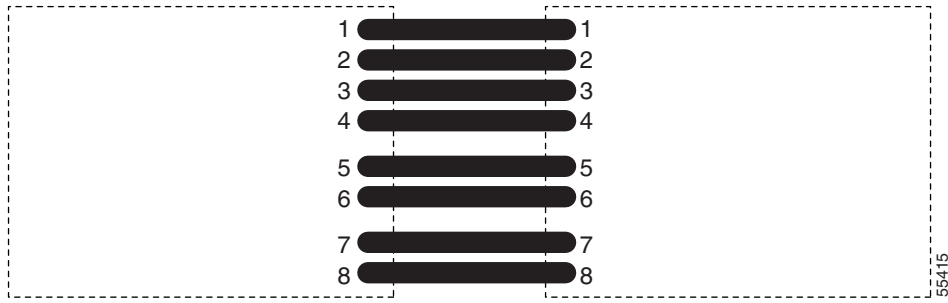


*Table 1-39   Lan Cable Pinout*

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

Figure 1-30 and Table 1-40 shows a cross-over cable layout and pinouts.

*Figure 1-30   Cross-over Cable Layout*
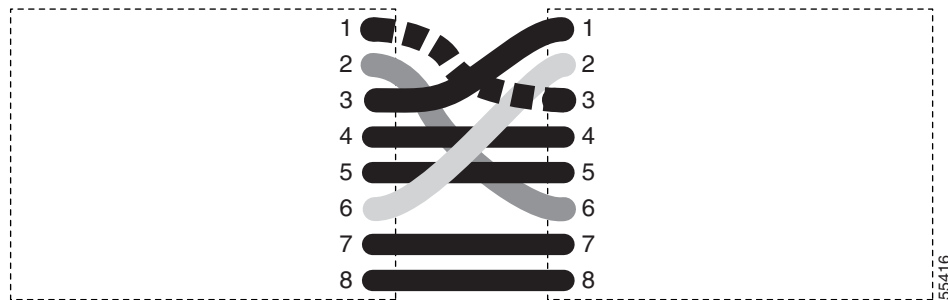


*Table 1-40   Cross-over Cable Pinout*

| 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 |

*Table 1-40    Cross-over Cable Pinout (continued)*

| Pin | Color | Pair | Name | Pin |
|-----|-------|------|------|-----|
| 6 | green | 3 | Receive Data - | 2 |
| 7 | white/brown | 4 | | 7 |
| 8 | brown | 4 | | 8 |

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

## 1.9.2.2  Replace Faulty GBIC or SFP Connectors

GBICs and SFPs are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

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

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

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities, see Table 1-41, Table 1-42, and refer to the *Cisco ONS 15454 Reference Manual*.

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

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G1000-4, or G1K-4 card. The other model has a locking handle. Both models are shown in Figure 1-31.

*Figure 1-31    Gigabit Interface Converters*
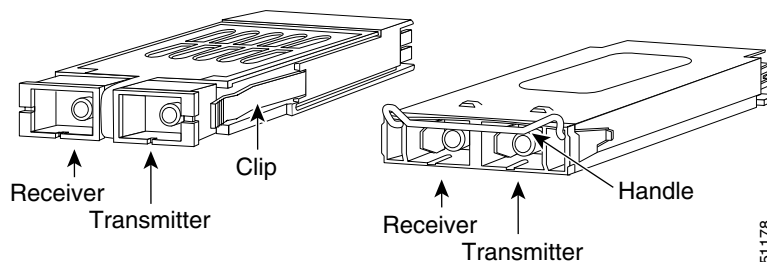


Table 1-41 shows the available GBICs.

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

*Table 1-41    Available GBICs*

| GBIC | Associated Cards | Application | Fiber | Product Number |
|------|------------------|-------------|-------|----------------|
| 1000BaseSX | E1000-2-G G1000-4 G1K-4 | Short reach | Multimode fiber up to 550 m long | 15454E-GBIC-SX= |
| 1000BaseLX | E1000-2-G G1000-4 G1K-4 | Long reach | Single-mode fiber up to 5 km long | 15454E-GBIC-LX= |
| 1000BaseZX | G1000-4 G1K-4 | Extra long reach | Single-mode fiber up to 70 km long | 15454E-GBIC-ZX= |

Table 1-42 on page 1-82 shows the available SFPs.

*Table 1-42    Available SFPs*

| SFP | Associated Cards | Application | Fiber | Product Number |
|-----|------------------|-------------|-------|----------------|
| 1000BaseSX | ML1000-2 | Short reach | Multimode fiber up to 550 m long | 15454E-SFP-LC-SX= |
| 1000BaseLX | ML1000-2 | Long reach | Single-mode fiber up to 5 km long | 15454E-SFP-LC-LX= |

## Procedure: Remove GBIC or SFP Connectors

**Step 1**  Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector.

**Warning**  **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

**Step 2**  Release the GBIC or SFP from the slot by simultaneously squeezing the two plastic tabs on each side.

**Step 3**  Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

## Procedure: Installing a GBIC with Clips

**Step 1**  Remove the GBIC from its protective packaging.

**Step 2**  Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

**Step 3**  Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

**Step 4**  Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G1000-4 card (shown in Figure 1-32).

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

*Figure 1-32   GBIC Installation (with Clips)*

Plug →

E1000
2

FAIL
ACT
SF

RX
1
TX

ACT/LINK

ACT/LINK

RX
2
TX

33678 12831

44734
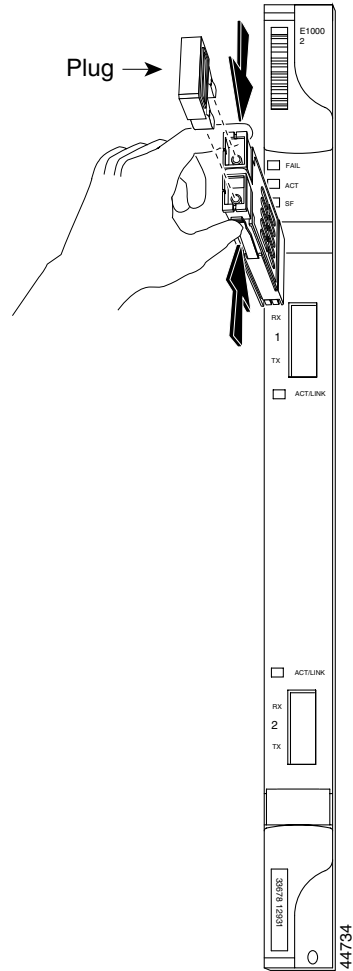
**Step 5**    Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

**Step 6**    When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

**Step 7**    Return to your originating procedure (NTP).

## Procedure: Installing a GBIC with a Handle

**Step 1**    Remove the GBIC from its protective packaging.

**Step 2**    Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

**Step 3**    Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

**Step 4**    Remove the protective plug from the SC-type connector.

**Step 5**    Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, G1K-4, or G1000-4 card.

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

**Step 6** Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.

**Step 7** Return to your originating procedure (NTP).

## 1.9.3  Optical Card Transmit and Receive Levels

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

*Table 1-43   Optical Card Transmit and Receive Levels*

| Optical Card | Receive | Transmit |
|---|---|---|
| OC3 IR 4/STM1SH 1310 | –28 to –8 dBm | –15 to –8 dBm |
| OC3 IR/STM 1SH 1310-8 | –30 to –8 dBm | –15 to –8 dBm |
| OC12 IR/STM4 SH 1310 | –28 to –8 dBm | –15 to –8 dBm |
| OC12 LR/STM4 LH 1310 | –28 to –8 dBm | –3 to +2 dBm |
| OC12 LR/STM4 LH 1550 | –28 to –8 dBm | –3 to +2 dBm |
| OC12 IR/STM4 SH 1310-4 | –28 to –8 dBm | –3 to +2 dBm |
| OC48 IR/STM16 SH AS 1310 | –18 to 0 dBm | –5 to 0 dBm |
| OC48 LR/STM16 LH AS 1550 | –28 to –8 dBm | –2 to +3 dBm |
| OC48 ELR/STM16 EH 100GHz | –28 to –8 dBm | –2 to 0 dBm |
| OC192 SR/STM64 IO 1310 | –11 to –1 dBm | –6 to –1 dBm |
| OC192 IR STM64 SH 1550 | –14 to –1 dBm | –1 to +2 dBm |
| OC192 LR/STM64 LH 1550 | –21 to –9 dBm | +7 to +10 dBm |
| OC192 LR/STM64 LH ITU 15xx.xx | –22 to –9 dBm | +3 to +6 dBm |
| TXP-MR-10G | | |
| Trunk side:<br>Client side: | –26 to –8 dBm<br>–14 to –1 dBm | –16 to +3 dBm<br>–6 to –1 dBm |
| MXP-2.5G-10G | | |
| Trunk side:<br>Client side: | –26 to –8 dBm<br>depends on SFP | –16 to +3 dBm<br>depends on SFP |

## 1.10  Power and LED Tests

This section provides symptoms and solutions for power supply problems, power consumption, and LED indicators.

# 1.10.1 Power Supply Problems

**Symptom**  Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

Table 1-44 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-44    Power Supply Problems*

| Possible Problem | Solution |
|---|---|
| Loss of power or low voltage. | The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. |
| Improperly connected power supply. | A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. |
| | A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General** tabs and change the *Date* and *Time* fields. |
| | See the "Isolate the Cause of Power Supply Problems" procedure on page 1-85. |

**Warning**    **When working with live power, always use proper tools and eye protection.**

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

**Caution**    Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

## Procedure: Isolate the Cause of Power Supply Problems

**Step 1**    If a single ONS 15454 show signs of fluctuating power or power loss:

    **a.** Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.

    **b.** Verify that the power cable is #12 or #14 AWG and in good condition.

    **c.** Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.

    **d.** Verify that 20 A fuses are used in the fuse panel.

    **e.** Verify that the fuses are not blown.

  **f.** Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.

  **g.** Verify that the DC power source has enough capacity to carry the power load.

  **h.** If the DC power source is battery-based:

   • Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.

   • Check the age of the batteries. Battery performance decreases with age.

   • Check for opens and shorts in batteries, which might affect power output.

   • If brownouts occur, the power load and fuses might be too high for the battery plant.

**Step 2** If multiple pieces of site equipment show signs of fluctuating power or power loss:

  **a.** Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.

  **b.** Check for excessive power drains caused by other equipment, such as generators.

  **c.** Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

## 1.10.2  Power Consumption for Node and Cards

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

Table 1-45 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-45   Power Consumption for Node and Cards*

| Possible Problem | Solution |
|---|---|
| Improper power supply. | Refer to power information in the *Cisco ONS 15454 Reference Manual*. |

## 1.10.3  Lamp Test for Card LEDs

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

Table 1-46 describes the potential cause(s) of the symptom and the solution(s).

*Table 1-46   Lamp Test for Card LEDs*

| Possible Problem | Solution |
|---|---|
| Faulty LED | A lamp test verifies that all the card LEDs work. Run this diagnostic test as part of the initial ONS 15454 turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. |
| | See the "Verify Card LED Operation" procedure on page 1-87. |

## 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.

**C H A P T E R** **2**

# Alarm Troubleshooting

---

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

---

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Table 2-1 on page 2-2 through Table 2-4 on page 2-3 give lists of ONS 15454 alarms organized by severity. Table 2-5 on page 2-5 gives a list of alarm organized alphabetically. Table 2-6 on page 2-7 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 15454 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 15454 alarms on unprovisioned card ports is Minor, Non-Service Affecting, as defined in Telcordia GR-474. All severities listed in the alarm entry are the default for the active card, if applicable. Alarm severities can be altered from default settings for individual alarms or groups of alarms on a card, node, or network basis.

---

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

---

### 2.1.1 Critical Alarms (CR)

Table 2-1 lists Critical alarms.

*Table 2-1    Critical Alarm Index*

| | | |
|---|---|---|
| AUTOLSROFF, page 2-30 | IMPROPRMVL, page 2-87 | MEA (BP), page 2-114 |
| BKUPMEMP, page 2-36 | LOF (DS-3), page 2-95 | MEA (EQPT), page 2-115 |
| CKTDOWN, page 2-43 | LOF (EC-N), page 2-96 | MEA (FAN), page 2-117 |
| COMIOXC, page 2-46 | LOF (OC-N), page 2-96 | MFGMEM, page 2-118 |
| CTNEQPT-PBPROT, page 2-50 | LOM, page 2-98 | OTUK-LOF, page 2-124 |
| CTNEQPT-PBWORK, page 2-52 | LOP-P, page 2-98 | PLM-P, page 2-128 |
| EQPT, page 2-59 | LOS (DS-3), page 2-102 | SWMTXMOD, page 2-150 |
| EQPT-MISS, page 2-60 | LOS (EC-N), page 2-103 | TIM-P, page 2-155 |
| FAN, page 2-70 | LOS (OC-N), page 2-105 | UNEQ-P, page 2-159 |
| HITEMP, page 2-86 | MEA (AIP), page 2-114 | |

## 2.1.2  Major Alarms (MJ)

Table 2-2 lists Major alarms.

*Table 2-2    Major Alarm Index*

| | | |
|---|---|---|
| APSCM, page 2-25 | E-W-MISMATCH, page 2-61 | PORT-COMM-FAIL, page 2-131 |
| APSCNMIS, page 2-26 | EXTRA-TRAF-PREEMPT, page 2-65 | PORT-MISMATCH, page 2-131 |
| BLSROSYNC, page 2-36 | FANDEGRADE, page 2-71 | PORT-MISSING, page 2-131 |
| CARLOSS (EQPT), page 2-37 | GCC-EOC, page 2-83 | PRC-DUPID, page 2-132 |
| CARLOSS (E-Series), page 2-38 | INVMACADR, page 2-90 | RCVR-MISS, page 2-135 |
| CARLOSS (G-Series), page 2-39 | LOF (BITS), page 2-93 | RING-MISMATCH, page 2-138 |
| CARLOSS (ML-Series), page 2-42 | LOF (DS-1), page 2-94 | SQUELCHED, page 2-146 |
| CONTBUS-A-18, page 2-47 | LOP-V, page 2-99 | SYSBOOT, page 2-155 |
| CONTBUS-B-18, page 2-47 | LOS (BITS), page 2-101 | TPTFAIL (G-Series), page 2-156 |
| CONTBUS-IO-A, page 2-48 | LOS (DS-1), page 2-101 | TPTFAIL (ML-Series), page 2-157 |
| CONTBUS-IO-B, page 2-49 | MEM-GONE, page 2-117 | TRMT, page 2-158 |
| DBOSYNC, page 2-54 | OTUK-IAE, page 2-124 | TRMT-MISS, page 2-158 |
| DSP-COMM-FAIL, page 2-55 | PEER-NORESPONSE, page 2-128 | UNEQ-V, page 2-161 |
| DSP-FAIL, page 2-55 | PORT-CODE-MISM, page 2-130 | WVL-MISMATCH, page 2-162 |
| EOC, page 2-57 | | |

## 2.1.3  Minor Alarms (MN)

Table 2-3 lists Minor alarms.

*Table 2-3      Minor Alarm Index*

| | | |
|---|---|---|
| APSB, page 2-23 | FEPRLF, page 2-79 | MEM-LOW, page 2-118 |
| APSCDFLTK, page 2-24 | FSTSYNC, page 2-82 | NOT-AUTHENTICATED, page 2-119 |
| APSC-IMP, page 2-24 | HI-LASERBIAS, page 2-83 | OTUK-TIM, page 2-125 |
| APSCINCON, page 2-25 | HI-LASERTEMP, page 2-84 | PLM-V, page 2-130 |
| APSMM, page 2-27 | HI-RXPOWER, page 2-84 | PROTNA, page 2-132 |
| AUTORESET, page 2-31 | HI-RXTEMP, page 2-85 | PWR-A, page 2-133 |
| AUTOSW-LOP (VTMON), page 2-32 | HITEMP, page 2-86 | PWR-B, page 2-134 |
| AUTOSW-LOP (VTMON), page 2-32 | HI-TXPOWER, page 2-86 | PWR-REDUN, page 2-134 |
| DATAFLT, page 2-53 | LASEREOL, page 2-91 | RSVP-HELLODOWN, page 2-138 |
| EHIBATVG-A, page 2-56 | LMP-HELLODOWN, page 2-92 | SFTWDOWN, page 2-143 |
| EHIBATVG-B, page 2-56 | LMP-NDFAIL, page 2-92 | SNTP-HOST, page 2-144 |
| ELWBATVG-A, page 2-56 | LO-LASERBIAS, page 2-97 | SSM-FAIL, page 2-147 |
| ELWBATVG-B, page 2-57 | LO-LASERTEMP, page 2-97 | SYNCPRI, page 2-153 |
| ERROR-CONFIG, page 2-60 | LO-RXPOWER, page 2-99 | SYNCSEC, page 2-154 |
| EXCCOL, page 2-63 | LO-RXTEMP, page 2-100 | SYNCTHIRD, page 2-154 |
| EXT, page 2-64 | LO-TXPOWER, page 2-106 | TIM-P, page 2-155 |

## 2.1.4  Conditions (NA or NR)

Table 2-4 lists Not Alarmed or Not Reported conditions.

*Table 2-4      Conditions Index*

| | | |
|---|---|---|
| AIS, page 2-21 | FE-MANWKSWPR-SPAN, page 2-79 | ODUK-SF-PM, page 2-122 |
| AIS-L, page 2-22 | FORCED-REQ, page 2-80 | ODUK-TIM-PM, page 2-122 |
| AIS-P, page 2-22 | FORCED-REQ-RING, page 2-80 | OTUK-AIS, page 2-123 |
| AIS-V, page 2-22 | FORCED-REQ-SPAN, page 2-81 | OTUK-BDI, page 2-123 |
| AS-CMD, page 2-28 | FRCDSWTOINT, page 2-81 | OTUK-SD, page 2-125 |
| AS-MT, page 2-29 | FRCDSWTOPRI, page 2-81 | OTUK-SF, page 2-125 |
| AUD-LOG-LOSS, page 2-29 | FRCDSWTOSEC, page 2-81 | PDI-P, page 2-126 |
| AUD-LOG-LOW, page 2-30 | FRCDSWTOTHIRD, page 2-82 | RAI, page 2-135 |
| AUTOSW-AIS, page 2-31 | FRNGSYNC, page 2-82 | RFI-L, page 2-136 |
| AUTOSW-LOP (STSMON), page 2-32 | FULLPASSTHR-BI, page 2-82 | RFI-P, page 2-136 |
| AUTOSW-PDI, page 2-32 | HLDOVRSYNC, page 2-87 | RFI-V, page 2-137 |
| AUTOSW-SDBER, page 2-33 | INC-ISD, page 2-89 | RING-SW-EAST, page 2-138 |
| AUTOSW-SFBER, page 2-33 | INHSWPR, page 2-89 | RING-SW-WEST, page 2-138 |
| AUTOSW-UNEQ (STSMON), page 2-34 | INHSWWKG, page 2-90 | RUNCFG-SAVENEED, page 2-139 |

*Table 2-4      Conditions Index (continued)*

| | | |
|---|---|---|
| BAT-A-HGH-VLT, page 2-34 | KB-PASSTHR, page 2-90 | SD, page 2-139 |
| BAT-A-LOW-VLT, page 2-35 | LAN-POL-REV, page 2-90 | SD-L, page 2-140 |
| BAT-B-HGH-VLT, page 2-35 | LKOUTPR-S, page 2-91 | SD-P, page 2-141 |
| BAT-B-LOW-VLT, page 2-35 | LOCKOUT-REQ, page 2-93 | SF, page 2-141 |
| CLDRESTART, page 2-45 | LOCKOUT-REQ-RING, page 2-93 | SF-L, page 2-142 |
| DS3-MISM, page 2-54 | LPBKCRS, page 2-107 | SF-P, page 2-142 |
| EXERCISE-RING-REQ, page 2-64 | LPBKDS1FEAC, page 2-107 | SPAN-SW-EAST, page 2-144 |
| EXERCISE-SPAN-REQ, page 2-64 | LPBKDS1FEAC-CMD, page 2-108 | SPAN-SW-WEST, page 2-144 |
| FAILTOSW, page 2-65 | LPBKDS3FEAC, page 2-108 | SQUELCH, page 2-145 |
| FAILTOSW-PATH, page 2-66 | LPBKDS3FEAC-CMD, page 2-108 | SSM-DUS, page 2-147 |
| FAILTOSWR, page 2-67 | LPBKFACILITY (DS-1 or DS-3), page 2-109 | SSM-LNC, page 2-147 |
| FAILTOSWS, page 2-68 | LPBKFACILITY (EC-N), page 2-109 | SSM-OFF, page 2-147 |
| FE-AIS, page 2-71 | LPBKFACILITY (OC-N), page 2-110 | SSM-PRC, page 2-148 |
| FE-DS1-MULTLOS, page 2-71 | LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 | SSM-PRS, page 2-148 |
| FE-DS1-NSA, page 2-72 | LPBKTERMINAL (G-Series), page 2-111 | SSM-RES, page 2-148 |
| FE-DS3-SA, page 2-74 | MAN-REQ, page 2-112 | SSM-SMC, page 2-148 |
| FE-DS1-SNGLLOS, page 2-73 | MANRESET, page 2-112 | SSM-ST2, page 2-149 |
| FE-DS3-NSA, page 2-73 | MANSWTOINT, page 2-112 | SSM-ST3, page 2-149 |
| FE-DS3-SA, page 2-74 | MANSWTOPRI, page 2-112 | SSM-ST3E, page 2-149 |
| FE-EQPT-NSA, page 2-74 | MANSWTOSEC, page 2-113 | SSM-ST4, page 2-149 |
| FE-EXERCISING-RING, page 2-75 | MANSWTOTHIRD, page 2-113 | SSM-STU, page 2-150 |
| FE-EXERCISING-SPAN, page 2-75 | MANUAL-REQ-RING, page 2-113 | SSM-TNC, page 2-150 |
| FE-FRCDWKSWPR-RING, page 2-75 | MANUAL-REQ-SPAN, page 2-113 | SWTOPRI, page 2-152 |
| FE-FRCDWKSWPR-SPAN, page 2-76 | NO-CONFIG, page 2-118 | SWTOSEC, page 2-152 |
| FE-IDLE, page 2-76 | ODUK-AIS-PM, page 2-119 | SWTOTHIRD, page 2-152 |
| FE-LOCKOUTOFPR-SPAN, page 2-77 | ODUK-BDI-PM, page 2-120 | SYNC-FREQ, page 2-153 |
| FE-LOF, page 2-77 | ODUK-LCK-PM, page 2-120 | UNC-WORD, page 2-159 |
| FE-LOS, page 2-78 | ODUK-OCI-PM, page 2-121 | WKSWPR, page 2-162 |
| FE-MANWKSWPR-RING, page 2-78 | ODUK-SD-PM, page 2-121 | WTR, page 2-162 |

## 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*

| | | |
|---|---|---|
| AIS, page 2-21 | FE-LOF, page 2-77 | ODUK-BDI-PM, page 2-120 |
| AIS-L, page 2-22 | FE-LOS, page 2-78 | ODUK-LCK-PM, page 2-120 |
| AIS-P, page 2-22 | FE-MANWKSWPR-RING, page 2-78 | ODUK-OCI-PM, page 2-121 |
| AIS-V, page 2-22 | FE-MANWKSWPR-SPAN, page 2-79 | ODUK-SD-PM, page 2-121 |
| APSB, page 2-23 | FEPRLF, page 2-79 | ODUK-SF-PM, page 2-122 |
| APSCDFLTK, page 2-24 | FORCED-REQ, page 2-80 | ODUK-TIM-PM, page 2-122 |
| APSC-IMP, page 2-24 | FORCED-REQ-RING, page 2-80 | OTUK-AIS, page 2-123 |
| APSCINCON, page 2-25 | FORCED-REQ-SPAN, page 2-81 | OTUK-BDI, page 2-123 |
| APSCM, page 2-25 | FRCDSWTOINT, page 2-81 | OTUK-IAE, page 2-124 |
| APSCNMIS, page 2-26 | FRCDSWTOPRI, page 2-81 | OTUK-LOF, page 2-124 |
| APSMM, page 2-27 | FRCDSWTOSEC, page 2-81 | OTUK-SD, page 2-125 |
| AS-CMD, page 2-28 | FRCDSWTOTHIRD, page 2-82 | OTUK-SF, page 2-125 |
| AS-MT, page 2-29 | FRNGSYNC, page 2-82 | OTUK-TIM, page 2-125 |
| AUD-LOG-LOSS, page 2-29 | FSTSYNC, page 2-82 | PDI-P, page 2-126 |
| AUD-LOG-LOW, page 2-30 | FULLPASSTHR-BI, page 2-82 | PEER-NORESPONSE, page 2-128 |
| AUTOLSROFF, page 2-30 | GCC-EOC, page 2-83 | PLM-P, page 2-128 |
| AUTORESET, page 2-31 | HI-LASERBIAS, page 2-83 | PLM-V, page 2-130 |
| AUTOSW-AIS, page 2-31 | HI-LASERTEMP, page 2-84 | PORT-CODE-MISM, page 2-130 |
| AUTOSW-LOP (STSMON), page 2-32 | HI-RXPOWER, page 2-84 | PORT-MISSING, page 2-131 |
| AUTOSW-LOP (VTMON), page 2-32 | HI-RXTEMP, page 2-85 | PORT-COMM-FAIL, page 2-131 |
| AUTOSW-PDI, page 2-32 | HITEMP, page 2-86 | PORT-MISMATCH, page 2-131 |
| AUTOSW-SDBER, page 2-33 | HI-TXPOWER, page 2-86 | PRC-DUPID, page 2-132 |
| AUTOSW-SFBER, page 2-33 | HLDOVRSYNC, page 2-87 | PROTNA, page 2-132 |
| AUTOSW-UNEQ (STSMON), page 2-34 | IMPROPRMVL, page 2-87 | PWR-A, page 2-133 |
| AUTOSW-UNEQ (VTMON), page 2-34 | INC-ISD, page 2-89 | PWR-B, page 2-134 |
| BAT-A-HGH-VLT, page 2-34 | INHSWPR, page 2-89 | PWR-REDUN, page 2-134 |
| BAT-A-LOW-VLT, page 2-35 | INHSWWKG, page 2-90 | RAI, page 2-135 |
| BAT-B-HGH-VLT, page 2-35 | INVMACADR, page 2-90 | RCVR-MISS, page 2-135 |
| BAT-B-LOW-VLT, page 2-35 | KB-PASSTHR, page 2-90 | RFI-L, page 2-136 |
| BKUPMEMP, page 2-36 | LAN-POL-REV, page 2-90 | RFI-P, page 2-136 |
| BLSROSYNC, page 2-36 | LASEREOL, page 2-91 | RFI-V, page 2-137 |
| CARLOSS (EQPT), page 2-37 | LKOUTPR-S, page 2-91 | RING-MISMATCH, page 2-138 |
| CARLOSS (E-Series), page 2-38 | LMP-HELLODOWN, page 2-92 | RING-SW-EAST, page 2-138 |
| CARLOSS (G-Series), page 2-39 | LMP-NDFAIL, page 2-92 | RING-SW-WEST, page 2-138 |
| CARLOSS (ML-Series), page 2-42 | LOCKOUT-REQ, page 2-93 | RSVP-HELLODOWN, page 2-138 |
| CKTDOWN, page 2-43 | LOCKOUT-REQ-RING, page 2-93 | RUNCFG-SAVENEED, page 2-139 |

*Table 2-5    Alphabetical Alarm Index (continued)*

| | | |
|---|---|---|
| CLDRESTART, page 2-45 | LOF (BITS), page 2-93 | SD, page 2-139 |
| COMIOXC, page 2-46 | LOF (DS-1), page 2-94 | SD-L, page 2-140 |
| CONTBUS-A-18, page 2-47 | LOF (DS-3), page 2-95 | SD-P, page 2-141 |
| CONTBUS-B-18, page 2-47 | LOF (EC-N), page 2-96 | SF, page 2-141 |
| CONTBUS-IO-A, page 2-48 | LOF (OC-N), page 2-96 | SF-L, page 2-142 |
| CONTBUS-IO-B, page 2-49 | LO-LASERBIAS, page 2-97 | SF-P, page 2-142 |
| CTNEQPT-PBPROT, page 2-50 | LO-LASERTEMP, page 2-97 | SFTWDOWN, page 2-143 |
| CTNEQPT-PBWORK, page 2-52 | LOM, page 2-98 | SNTP-HOST, page 2-144 |
| DATAFLT, page 2-53 | LOP-P, page 2-98 | SPAN-SW-EAST, page 2-144 |
| DBOSYNC, page 2-54 | LOP-V, page 2-99 | SPAN-SW-WEST, page 2-144 |
| DS3-MISM, page 2-54 | LO-RXPOWER, page 2-99 | SQUELCH, page 2-145 |
| DSP-COMM-FAIL, page 2-55 | LO-RXTEMP, page 2-100 | SQUELCHED, page 2-146 |
| DSP-FAIL, page 2-55 | LOS (BITS), page 2-101 | SSM-DUS, page 2-147 |
| EHIBATVG-A, page 2-56 | LOS (DS-1), page 2-101 | SSM-FAIL, page 2-147 |
| EHIBATVG-B, page 2-56 | LOS (DS-3), page 2-102 | SSM-LNC, page 2-147 |
| ELWBATVG-A, page 2-56 | LOS (EC-N), page 2-103 | SSM-OFF, page 2-147 |
| ELWBATVG-B, page 2-57 | LOS (OC-N), page 2-105 | SSM-PRC, page 2-148 |
| EOC, page 2-57 | LO-TXPOWER, page 2-106 | SSM-PRS, page 2-148 |
| EQPT, page 2-59 | LPBKCRS, page 2-107 | SSM-RES, page 2-148 |
| EQPT-MISS, page 2-60 | LPBKDS1FEAC, page 2-107 | SSM-SMC, page 2-148 |
| ERROR-CONFIG, page 2-60 | LPBKDS1FEAC-CMD, page 2-108 | SSM-ST2, page 2-149 |
| E-W-MISMATCH, page 2-61 | LPBKDS3FEAC, page 2-108 | SSM-ST3, page 2-149 |
| EXCCOL, page 2-63 | LPBKDS3FEAC-CMD, page 2-108 | SSM-ST3E, page 2-149 |
| EXERCISE-RING-REQ, page 2-64 | LPBKFACILITY (DS-1 or DS-3), page 2-109 | SSM-ST4, page 2-149 |
| EXERCISE-SPAN-REQ, page 2-64 | LPBKFACILITY (EC-N), page 2-109 | SSM-STU, page 2-150 |
| EXT, page 2-64 | LPBKFACILITY (OC-N), page 2-110 | SSM-TNC, page 2-150 |
| EXTRA-TRAF-PREEMPT, page 2-65 | LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 | SWMTXMOD, page 2-150 |
| FAILTOSW, page 2-65 | LPBKTERMINAL (G-Series), page 2-111 | SWTOPRI, page 2-152 |
| FAILTOSW-PATH, page 2-66 | MAN-REQ, page 2-112 | SWTOSEC, page 2-152 |
| FAILTOSWR, page 2-67 | MANRESET, page 2-112 | SWTOTHIRD, page 2-152 |
| FAILTOSWS, page 2-68 | MANSWTOINT, page 2-112 | SYNC-FREQ, page 2-153 |
| FAN, page 2-70 | MANSWTOPRI, page 2-112 | SYNCPRI, page 2-153 |
| FANDEGRADE, page 2-71 | MANSWTOSEC, page 2-113 | SYNCSEC, page 2-154 |
| FE-AIS, page 2-71 | MANSWTOTHIRD, page 2-113 | SYNCTHIRD, page 2-154 |
| FE-DS1-MULTLOS, page 2-71 | MANUAL-REQ-RING, page 2-113 | SYSBOOT, page 2-155 |

***Table 2-5     Alphabetical Alarm Index (continued)***

| | | |
|---|---|---|
| FE-DS1-NSA, page 2-72 | MANUAL-REQ-SPAN, page 2-113 | TIM-P, page 2-155 |
| FE-DS1-SA, page 2-72 | MEA (AIP), page 2-114 | TPTFAIL (G-Series), page 2-156 |
| FE-DS1-SNGLLOS, page 2-73 | MEA (BP), page 2-114 | TPTFAIL (ML-Series), page 2-157 |
| FE-DS3-NSA, page 2-73 | MEA (EQPT), page 2-115 | TRMT, page 2-158 |
| FE-DS3-NSA, page 2-73 | MEA (FAN), page 2-117 | TRMT-MISS, page 2-158 |
| FE-EQPT-NSA, page 2-74 | MEM-GONE, page 2-117 | UNC-WORD, page 2-159 |
| FE-EXERCISING-RING, page 2-75 | MEM-LOW, page 2-118 | UNEQ-P, page 2-159 |
| FE-EXERCISING-SPAN, page 2-75 | MFGMEM, page 2-118 | UNEQ-V, page 2-161 |
| FE-FRCDWKSWPR-RING, page 2-75 | NO-CONFIG, page 2-118 | WKSWPR, page 2-162 |
| FE-FRCDWKSWPR-SPAN, page 2-76 | NOT-AUTHENTICATED, page 2-119 | WTR, page 2-162 |
| FE-IDLE, page 2-76 | ODUK-AIS-PM, page 2-119 | WVL-MISMATCH, page 2-162 |
| FE-LOCKOUTOFPR-SPAN, page 2-77 | | |

# 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***

| |
|---|
| AEP: EQPT, page 2-59 |
| AEP: MFGMEM, page 2-118 |
| AIP: INVMACADR, page 2-90 |
| AIP: MEA (AIP), page 2-114 |
| AIP: MFGMEM, page 2-118 |
| BITS: LOS (BITS), page 2-101 |
| BITS: AIS, page 2-21 |
| BITS: LOF (BITS), page 2-93 |
| BITS: SSM-DUS, page 2-147 |
| BITS: SSM-FAIL, page 2-147 |
| BITS: SSM-OFF, page 2-147 |
| BITS: SSM-PRS, page 2-148 |
| BITS: SSM-RES, page 2-148 |
| BITS: SSM-SMC, page 2-148 |
| BITS: SSM-ST2, page 2-149 |
| BITS: SSM-ST3, page 2-149 |
| BITS: SSM-ST3E, page 2-149 |
| BITS: SSM-ST4, page 2-149 |
| BITS: SSM-STU, page 2-150 |

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

| |
|---|
| BITS: SSM-TNC, page 2-150 |
| BP: AS-CMD, page 2-28 |
| BP: MEA (BP), page 2-114 |
| BP: MFGMEM, page 2-118 |
| CC: LMP-HELLODOWN, page 2-92 |
| CC: LMP-NDFAIL, page 2-92 |
| CKT: CKTDOWN, page 2-43 |
| DS1: AIS, page 2-21 |
| DS1: AS-CMD, page 2-28 |
| DS1: AS-MT, page 2-29 |
| DS1: LOF (DS-1), page 2-94 |
| DS1: LOS (DS-1), page 2-101 |
| DS1: LPBKDS1FEAC, page 2-107 |
| DS1: LPBKDS1FEAC-CMD, page 2-108 |
| DS1: LPBKFACILITY (DS-1 or DS-3), page 2-109 |
| DS1: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 |
| DS1: RAI, page 2-135 |
| DS1: RCVR-MISS, page 2-135 |
| DS3: SD, page 2-139 |
| DS3: SF, page 2-141 |
| DS1: TRMT, page 2-158 |
| DS1: TRMT-MISS, page 2-158 |
| DS3: AIS, page 2-21 |
| DS3: AS-CMD, page 2-28 |
| DS3: AS-MT, page 2-29 |
| DS3: DS3-MISM, page 2-54 |
| DS3: FE-AIS, page 2-71 |
| DS3: FE-DS1-MULTLOS, page 2-71 |
| DS3: FE-DS1-NSA, page 2-72 |
| DS3: FE-DS1-SA, page 2-72 |
| DS3: FE-DS1-SNGLLOS, page 2-73 |
| DS3: FE-DS3-NSA, page 2-73 |
| DS3: FE-DS3-SA, page 2-74 |
| DS3: FE-EQPT-NSA, page 2-74 |
| DS3: FE-IDLE, page 2-76 |
| DS3: FE-LOF, page 2-77 |
| DS3: FE-LOS, page 2-78 |

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

| |
|---|
| DS3: INC-ISD, page 2-89 |
| DS3: LOF (DS-3), page 2-95 |
| DS3: LOS (DS-3), page 2-102 |
| DS3: LPBKDS1FEAC, page 2-107 |
| DS3: LPBKDS3FEAC, page 2-108 |
| DS3: LPBKDS3FEAC-CMD, page 2-108 |
| DS3: LPBKFACILITY (DS-1 or DS-3), page 2-109 |
| DS3: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 |
| DS3: RAI, page 2-135 |
| DWDM Client: AIS, page 2-21 |
| DWDM Client: AS-CMD, page 2-28 |
| DWDM Client: AS-MT, page 2-29 |
| DWDM Client: AUTOLSROFF, page 2-30 |
| DWDM Client: CARLOSS (ML-Series), page 2-42 |
| DWDM Client: FAILTOSW, page 2-65 |
| DWDM Client: EOC, page 2-57 |
| DWDM Client: FORCED-REQ-SPAN, page 2-81 |
| DWDM Client: HI-LASERBIAS, page 2-83 |
| DWDM Client: HI-LASERTEMP, page 2-84 |
| DWDM Client: HI-RXPOWER, page 2-84 |
| DWDM Client: HI-TXPOWER, page 2-86 |
| DWDM Client: LOCKOUT-REQ, page 2-93 |
| DWDM Client: LOF (OC-N), page 2-96 |
| DWDM Client: LO-LASERBIAS, page 2-97 |
| DWDM Client: LO-LASERTEMP, page 2-97 |
| DWDM Client: LO-RXPOWER, page 2-99 |
| DWDM Client: LO-TXPOWER, page 2-106 |
| DWDM Client: LOS (OC-N), page 2-105 |
| DWDM Client: LPBKFACILITY (OC-N), page 2-110 |
| DWDM Client: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 |
| DWDM Client: MANUAL-REQ-SPAN, page 2-113 |
| DWDM Client: PORT-CODE-MISM, page 2-130 |
| DWDM Client: PORT-COMM-FAIL, page 2-131 |
| DWDM Client: PORT-MISMATCH, page 2-131 |
| DWDM Client: PORT-MISSING, page 2-131 |
| DWDM Client: RFI-L, page 2-136 |
| DWDM Client: SD, page 2-139 |

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

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

| |
|---|
| DWDM Trunk: LO-RXTEMP, page 2-100 |
| DWDM Trunk: LOS (OC-N), page 2-105 |
| DWDM Trunk: LO-TXPOWER, page 2-106 |
| DWDM Trunk: LPBKFACILITY (EC-N), page 2-109 |
| DWDM Trunk: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110 |
| DWDM Trunk: ODUK-AIS-PM, page 2-119 |
| DWDM Trunk: ODUK-BDI-PM, page 2-120 |
| DWDM Trunk: ODUK-LCK-PM, page 2-120 |
| DWDM Trunk: ODUK-OCI-PM, page 2-121 |
| DWDM Trunk: ODUK-SD-PM, page 2-121 |
| DWDM Trunk: ODUK-SF-PM, page 2-122 |
| DWDM Trunk: ODUK-TIM-PM, page 2-122 |
| DWDM Trunk: OTUK-AIS, page 2-123 |
| DWDM Trunk: OTUK-BDI, page 2-123 |
| DWDM Trunk: OTUK-IAE, page 2-124 |
| DWDM Trunk: OTUK-LOF, page 2-124 |
| DWDM Trunk: OTUK-SD, page 2-125 |
| DWDM Trunk: OTUK-SF, page 2-125 |
| DWDM Trunk: OTUK-TIM, page 2-125 |
| DWDM Trunk: RFI-L, page 2-136 |
| DWDM Trunk: SD, page 2-139 |
| DWDM Trunk: SF, page 2-141 |
| DWDM Trunk: SQUELCHED, page 2-146 |
| DWDM Trunk: SSM-DUS, page 2-147 |
| DWDM Trunk: SSM-FAIL, page 2-147 |
| DWDM Trunk: SSM-LNC, page 2-147 |
| DWDM Trunk: SSM-OFF, page 2-147 |
| DWDM Trunk: SSM-PRC, page 2-148 |
| DWDM Trunk: SSM-PRS, page 2-148 |
| DWDM Trunk: SSM-RES, page 2-148 |
| DWDM Trunk: SSM-SMC, page 2-148 |
| DWDM Trunk: SSM-ST2, page 2-149 |
| DWDM Trunk: SSM-ST3, page 2-149 |
| DWDM Trunk: SSM-ST3E, page 2-149 |
| DWDM Trunk: SSM-ST4, page 2-149 |
| DWDM Trunk: SSM-STU, page 2-150 |
| DWDM Trunk: SSM-TNC, page 2-150 |

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

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

| |
|---|
| EQPT: MEM-GONE, page 2-117 |
| EQPT: MEM-LOW, page 2-118 |
| EQPT: NO-CONFIG, page 2-118 |
| EQPT: PEER-NORESPONSE, page 2-128 |
| EQPT: PROTNA, page 2-132 |
| EQPT: PWR-REDUN, page 2-134 |
| EQPT: RUNCFG-SAVENEED, page 2-139 |
| EQPT: SFTWDOWN, page 2-143 |
| EQPT: SWMTXMOD, page 2-150 |
| EQPT: WKSWPR, page 2-162 |
| EQPT: WTR, page 2-162 |
| ETHER: AS-CMD, page 2-28 |
| ETHER: CARLOSS (E-Series), page 2-38 |
| ETHER: CARLOSS (G-Series), page 2-39 |
| EXTSYNCH: FRCDSWTOPRI, page 2-81 |
| EXTSYNCH: FRCDSWTOSEC, page 2-81 |
| EXTSYNCH: FRCDSWTOTHIRD, page 2-82 |
| EXTSYNCH: MANSWTOPRI, page 2-112 |
| EXTSYNCH: MANSWTOSEC, page 2-113 |
| EXTSYNCH: MANSWTOTHIRD, page 2-113 |
| EXTSYNCH: SWTOPRI, page 2-152 |
| EXTSYNCH: SWTOSEC, page 2-152 |
| EXTSYNCH: SWTOTHIRD, page 2-152 |
| EXTSYNCH: SYNCPRI, page 2-153 |
| EXTSYNCH: SYNCSEC, page 2-154 |
| EXTSYNCH: SYNCTHIRD, page 2-154 |
| FAN: EQPT-MISS, page 2-60 |
| FAN: FAN, page 2-70 |
| FAN: FANDEGRADE, page 2-71 |
| FAN: MEA (FAN), page 2-117 |
| FAN: MFGMEM, page 2-118 |
| FUDC: AIS, page 2-21 |
| FUDC: LOS (OC-N), page 2-105 |
| HDGE [G1000]: AS-CMD, page 2-28 |
| HDGE [G1000]: AS-MT, page 2-29 |
| HDGE [G1000]: CARLOSS (G-Series), page 2-39 |
| HDGE [G1000]: LPBKTERMINAL (G-Series), page 2-111 |

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

| |
|---|
| HDGE [G1000]: TPTFAIL (G-Series), page 2-156 |
| ML1000: AS-CMD, page 2-28 |
| ML1000: CARLOSS (ML-Series), page 2-42 |
| ML1000: TPTFAIL (ML-Series), page 2-157 |
| MSUDC: AIS, page 2-21 |
| MSUDC: LOS (OC-N), page 2-105 |
| NBR: RSVP-HELLODOWN, page 2-138 |
| NE: AS-CMD, page 2-28 |
| NE: AUD-LOG-LOSS, page 2-29 |
| NE: AUD-LOG-LOW, page 2-30 |
| NE: BAT-A-HGH-VLT, page 2-34 |
| NE: BAT-A-LOW-VLT, page 2-35 |
| NE: BAT-B-HGH-VLT, page 2-35 |
| NE: BAT-B-LOW-VLT, page 2-35 |
| NE: DATAFLT, page 2-53 |
| NE: DBOSYNC, page 2-54 |
| NE: EHIBATVG-A, page 2-56 |
| NE: EHIBATVG-B, page 2-56 |
| NE: ELWBATVG-A, page 2-56 |
| NE: ELWBATVG-B, page 2-57 |
| NE: HITEMP, page 2-86 |
| NE: LAN-POL-REV, page 2-90 |
| NE: PRC-DUPID, page 2-132 |
| NE: PWR-A, page 2-133 |
| NE: PWR-B, page 2-134 |
| NE: SNTP-HOST, page 2-144 |
| NE: SYSBOOT, page 2-155 |
| NERING: BLSROSYNC, page 2-36 |
| NERING: FULLPASSTHR-BI, page 2-82 |
| NERING: KB-PASSTHR, page 2-90 |
| NERING: PRC-DUPID, page 2-132 |
| NERING: RING-MISMATCH, page 2-138 |
| NESYNCH: FRCDSWTOINT, page 2-81 |
| NESYNCH: FRCDSWTOPRI, page 2-81 |
| NESYNCH: FRCDSWTOSEC, page 2-81 |
| NESYNCH: FRCDSWTOTHIRD, page 2-82 |
| NESYNCH: FRNGSYNC, page 2-82 |

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

| |
|---|
| NESYNCH: FSTSYNC, page 2-82 |
| NESYNCH: HLDOVRSYNC, page 2-87 |
| NESYNCH: MANSWTOINT, page 2-112 |
| NESYNCH: MANSWTOPRI, page 2-112 |
| NESYNCH: MANSWTOSEC, page 2-113 |
| NESYNCH: MANSWTOTHIRD, page 2-113 |
| NESYNCH: SSM-PRS, page 2-148 |
| NESYNCH: SSM-RES, page 2-148 |
| NESYNCH: SSM-SMC, page 2-148 |
| NESYNCH: SSM-ST2, page 2-149 |
| NESYNCH: SSM-ST3, page 2-149 |
| NESYNCH: SSM-ST3E, page 2-149 |
| NESYNCH: SSM-ST4, page 2-149 |
| NESYNCH: SSM-STU, page 2-150 |
| NESYNCH: SSM-TNC, page 2-150 |
| NESYNCH: SWTOPRI, page 2-152 |
| NESYNCH: SWTOSEC, page 2-152 |
| NESYNCH: SWTOTHIRD, page 2-152 |
| NESYNCH: SYNCPRI, page 2-153 |
| NESYNCH: SYNCSEC, page 2-154 |
| NESYNCH: SYNCTHIRD, page 2-154 |
| OCN: AIS-L, page 2-22 |
| OCN: APSB, page 2-23 |
| OCN: APSCDFLTK, page 2-24 |
| OCN: APSC-IMP, page 2-24 |
| OCN: APSCINCON, page 2-25 |
| OCN: APSCM, page 2-25 |
| OCN: APSCNMIS, page 2-26 |
| OCN: APSMM, page 2-27 |
| OCN: AS-CMD, page 2-28 |
| OCN: AS-MT, page 2-29 |
| OCN: AUTOLSROFF, page 2-30 |
| OCN: EOC, page 2-57 |
| OCN: E-W-MISMATCH, page 2-61 |
| OCN: EXERCISE-RING-REQ, page 2-64 |
| OCN: EXERCISE-SPAN-REQ, page 2-64 |
| OCN: EXTRA-TRAF-PREEMPT, page 2-65 |

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

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

| |
|---|
| OCN: SSM-ST2, page 2-149 |
| OCN: SSM-ST3, page 2-149 |
| OCN: SSM-ST3E, page 2-149 |
| OCN: SSM-ST4, page 2-149 |
| OCN: SSM-STU, page 2-150 |
| OCN: SSM-TNC, page 2-150 |
| OCN: SYNC-FREQ, page 2-153 |
| OCN: WKSWPR, page 2-162 |
| OCN: WTR, page 2-162 |
| STSMON: AIS-P, page 2-22 |
| STSMON: AUTOSW-AIS, page 2-31 |
| STSMON: AUTOSW-LOP (STSMON), page 2-32 |
| STSMON: AUTOSW-PDI, page 2-32 |
| STSMON: AUTOSW-SDBER, page 2-33 |
| STSMON: AUTOSW-SFBER, page 2-33 |
| STSMON: AUTOSW-UNEQ (STSMON), page 2-34 |
| STSMON: FAILTOSW-PATH, page 2-66 |
| STSMON: FORCED-REQ, page 2-80 |
| STSMON: LOCKOUT-REQ, page 2-93 |
| STSMON: LOP-P, page 2-98 |
| STSMON: LPBKCRS, page 2-107 |
| STSMON: MAN-REQ, page 2-112 |
| STSMON: PDI-P, page 2-126 |
| STSMON: PLM-P, page 2-128 |
| STSMON: RFI-P, page 2-136 |
| STSMON: SD-P, page 2-141 |
| STSMON: SF-P, page 2-142 |
| STSMON: TIM-P, page 2-155 |
| STSMON: UNEQ-P, page 2-159 |
| STSMON: WKSWPR, page 2-162 |
| STSMON: WTR, page 2-162 |
| STSTERM: AIS-P, page 2-22 |
| STSTERM: LOP-P, page 2-98 |
| STSTERM: PDI-P, page 2-126 |
| STSTERM: PLM-P, page 2-128 |
| STSTERM: RFI-P, page 2-136 |
| STSTERM: SD-P, page 2-141 |

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

| |
| --- |
| STSTERM: SF-P, page 2-142 |
| STSTERM: TIM-P, page 2-155 |
| STSTERM: UNEQ-P, page 2-159 |
| VT-MON: AIS-V, page 2-22 |
| VT-MON: AUTOSW-AIS, page 2-31 |
| VT-MON: AUTOSW-LOP (VTMON), page 2-32 |
| VT-MON: AUTOSW-UNEQ (VTMON), page 2-34 |
| VT-MON: FAILTOSW-PATH, page 2-66 |
| VT-MON: FORCED-REQ, page 2-80 |
| VT-MON: LOCKOUT-REQ, page 2-93 |
| VT-MON: LOP-V, page 2-99 |
| VT-MON: MAN-REQ, page 2-112 |
| VT-MON: UNEQ-V, page 2-161 |
| VT-MON: WKSWPR, page 2-162 |
| VT-MON: WTR, page 2-162 |
| VT-TERM: AIS-V, page 2-22 |
| VT-TERM: PLM-V, page 2-130 |
| VT-TERM: RFI-V, page 2-137 |
| VT-TERM: SD-P, page 2-141 |
| VT-TERM: SF-P, page 2-142 |
| VT-TERM: UNEQ-V, page 2-161 |

## 2.3.1  Alarm Type/Object Definition

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

*Table 2-7    Alarm Type/Object Definition*

| | |
| --- | --- |
| **AEP** | Alarm expansion panel |
| **AIP** | Auxiliary interface protection module |
| **BITS** | Building integration timing supply (BITS) incoming references (BITS-1, BITS-2) |
| **BP** | The backplane |
| **CC** | Unified control plane (UCP) communication channel |
| **CKT** | UCP circuit |
| **DS1** | A DS-1 line a DS-1 card |
| **DS3** |  A DS-3 line on a DS-3 card |
| **ECN** | An EC-N line on an EC-N card |
| **DWDM Client** | The port (such as OC-12 or OC-48) where the client signal is plugged in |

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

| | |
|---|---|
| **DWDM Trunk** | The main span of the link; from the card point of view, it is the port operating in the 100-GHz spacing frequency grid |
| **ENV** | An environmental alarm port |
| **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 (CAT-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 G1000-4 cards. |
| **ML1000** | ML-Series Ethernet (traffic) cards |
| **MSUDC** | SONET Multiplex Section User Data Channel |
| **NBR** | UCP neighbor |
| **NE** | The entire network element |
| **NERING** | Represents the ring status in the NE |
| **NE-SYNCH** | Represents the timing status of the NE |
| **OCN** | An OC-N line on an OC-N 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 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 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). Conditions notify the user of an event which does not require action, such as a SWTOSEC or a MANRESET.

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 is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a port on an active DS-1 card is removed. This affects a provided service because traffic switches to the protect card. HITEMP 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 15454 also sends an AIS downstream. When it receives the AIS, the receiving node sends an RFI-L upstream. AIS-L 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 15454 uses Tecordia 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-192 card, a Critical alarm, over one hundred thousand DS-0 circuits lose protection.

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

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

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

# 2.5 Safety Summary

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

⚠
**Caution**    Hazardous voltage or energy might be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of OC-192 cards, in these instances users should pay close attention to the following warnings:

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

**Warning**    **Invisible laser radiation 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're 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 15454 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), page 2-105, 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 condition means there is an error in the SONET overhead at the line layer. The AIS-L condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service (IS) but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS or has an 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 2-21.

**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 condition means there is an error in the SONET overhead at the path layer. The AIS-P condition is secondary to another alarm occurring simultaneously in an upstream node. The AIS is caused by an incomplete circuit path, for example, when the port on the reporting node is in service (IS), but a node upstream on the circuit does not have its port in service. The upstream node often reports an LOS (OC-N), page 2-105, or has an out of service (OOS) OC-N port. 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 2-21.

**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, 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), page 2-105, or has an out of service (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, page 2-22, on the cross connected OC-N card.

**Note**    See the "AIS-V on DS3XM-6 Unused VT Circuits" section on page 1-71.

## Procedure:  Clear the AIS-V Condition

**Step 1**    Complete the "Clear the AIS Condition" procedure on page 2-21.

**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 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 15454. These invalid codes causes an APSB on an ONS node.

## Procedure:  Clear the APSB Alarm

**Step 1**    Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes.

For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454.

**Step 2**    If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly.

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

Step 3    If the alarm does not clear, log 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 alarm occurs when a bidirectional line switched ring (BLSR) is not properly configured, for example, when a four-node BLSR has one node configured as a path protection configuration. A node in a path protection configuration or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for BLSROSYNC, page 2-36.

### Procedure:  Clear the APSCDFLTK Alarm

Step 1    Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164 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 2-164 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 2-61.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 Procedure Guide* provides a procedure for fibering BLSRs.

Step 5    If the alarm does not clear and if the network is a four-fiber BLSR, 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 2-165.

Step 7    If nodes are not visible, complete the "Verify or Create Node DCC Terminations" procedure on page 2-165 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 alarm indicates invalid K bytes. The APSC-IMP alarm occurs on OC-N cards in a BLSR configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. APSCIMP occurs when these bits indicate a bad or invalid K byte. The alarm clears when the node receives valid K bytes.

⚠

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

## Procedure: Clear the APSC-IMP Alarm

**Step 1**    Use an optical test set to determine the validity of the K byte signal by examining the received signal.

For specific procedures to use the test set equipment, consult the manufacturer.

If the K byte is invalid, the problem is with upstream equipment and not in the reporting ONS 15454. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454s, consult the appropriate user documentation.

**Step 2**    If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs. Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164.

**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 2-164.

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

## Procedure: Clear the APSCINCON Alarm

**Step 1**    Look for other alarms, especially LOS (OC-N), page 2-105; LOF (OC-N), page 2-96, or AIS, page 2-21. Clearing these alarms clears the APSCINCON alarm.

**Step 2**    If an APSINCON alarm occurs with no other alarms, log onto http://www.cisco.com/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 alarm occurs when the ONS 15454 expects a working channel but receives a protection channel. In many cases, the working and protection channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm occurs only on the ONS 15454 when bidirectional protection is used on OC-N cards in a 1+1 configuration.

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

**Warning** **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the APSCM Alarm

**Step 1**  Verify that the working-card channel fibers are physically connected directly to the adjoining node's working-card channel fibers.

**Step 2**  If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node's protection-card channel fibers.

**Step 3**  If the alarm does not clear, log 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 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 2-164 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 2-164 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 15454 to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

**Step 5**    If the alarm does not clear, use the "Lock Out a BLSR Span" procedure on page 2-165 to lock out the span.

**Step 6**    Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165 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 alarm occurs when there is a mismatch of the protection switching schemes at the two ends of the span. If one node is provisioned for bidirectional switching, the node at the other end of the span must also be provisioned for bidirectional switching. If one end is provisioned for bidirectional and the other is provisioned for unidirectional, an APSMM alarm occurs in the ONS node that is provisioned for bidirectional. The APSMM alarm occurs in a 1+1 configuration.

### Procedure:  Clear the APSMM Alarm

**Step 1**    For the reporting ONS 15454, display the 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 condition applies to the network element (NE, or node),
backplane, and cards. It occurs when alarms are suppressed for one or more cards or for the entire shelf.

### Procedure:  Clear the AS-CMD Condition

**Step 1**   In the 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, note what entity the condition is reported against, such as a port, slot, or shelf.

If the condition is reported against a slot and card, alarms were either suppressed for the entire card or
for one of the ports. Note the slot number and continue with Step 3.

If the condition is reported against the backplane, go to Step 7.

If the condition is reported against a "system," go to Step 8.

**Step 3**   If the AS-CMD condition is reported for a card, determine whether alarms are suppressed for a port and
if so, raise the suppressed alarms:

**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 it and click **Apply**.

- If the Suppress Alarms column check box is not checked for a port row, click
**View > Go to Previous View**.

**Step 4**   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 backplane, the alarms are suppressed for cards such as the AIP that
are not in the optical or electrical slots. To clear the alarm:

**a.**   In node view, click the **Provisioning > Alarm Behavior** tabs.

**b.**   In the Backplane row, deselect the Suppress Alarms column check box.

**c.**   Click **Apply**.

**Step 8**   If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:

**a.**   In node view, click the **Provisioning > Alarm Behavior** tabs.

**b.**   Click the Suppress Alarms check box located at the bottom of the window to deselect the option.

**c.**   Click **Apply**.

**Step 9**    If the condition does not clear, log onto http://www.cisco.com/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 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 2-167.

**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 condition occurs when the log is 100% 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 the node view, click the **Maintenance > Audit** tabs.

**Step 2**    Click **Retrieve**.

**Step 3**    Click **Archive**.

**Step 4**    In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

**Step 5**    Enter a name in the File Name field.

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

**Step 6**    Click **Save**.

The 640 entries will be saved in this file. New entries will continue with the next number in the sequence, rather than starting over.

**Step 7**    If the alarm does not clear, log onto http://www.cisco.com/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 Loss condition occurs when the audit trail log is 80% full.

**Note** AUD-LOG-LOW is an informational condition. It does not require troubleshooting.

## 2.6.16 AUTOLSROFF

- Critical (CR), Service Affecting (SA)

The Auto Laser Shutdown alarm occurs when the OC-192 card temperature exceeds 194° F (90 ° C). The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.

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

**Warning** **Invisible laser radiation 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 AUTOLSROFF Alarm

**Step 1** View the temperature displayed on the ONS 15454 LCD front panel. For an illustration of the LCD panel, refer to the "View Alarm Counts on the LCD for a Slot or Port" procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 2** If the temperature of the shelf exceeds 194° F (90° C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-86.

**Step 3** If the temperature of the shelf is under 194° F (90° C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Card" procedure on page 2-169 for the OC-192 card.

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

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

**Step 4**  If card replacement does not clear the alarm, call the Technical Assistance Center (TAC) at 1-800-553-2447 to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

## 2.6.17  AUTORESET

- Minor (MN), Non-Service Affecting (NSA)

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

⚠️

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

### Procedure:  Clear the AUTORESET Alarm

**Step 1**  Verify that 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 2-169.

⚠️

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

✎

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

**Step 3**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.18  AUTOSW-AIS

- Not Reported (NR), Non-Service Affecting (NSA)

The Automatic path protection configuration Switch Caused by AIS condition indicates that automatic path protection configuration protection switching occurred because of an AIS condition. The path protection configuration is configured for revertive switching and reverts 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 2-21.

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 (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic path protection configuration Switch Caused by Loss of Pointer (LOP) condition indicates that automatic path protection configuration protection switching occurred because of an LOP-P, page 2-98. The path protection configuration is configured for revertive switching and reverts 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 2-98.

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).

# 2.6.20  AUTOSW-LOP (VTMON)

- Minor (MN), Service Affecting (SA)

The AUTOSW-LOP alarm indicates that automatic path protection configuration protection switching occurred because of an LOP-V, page 2-99. The path protection configuration is configured for revertive switching and reverts 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 2-99.

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).

# 2.6.21  AUTOSW-PDI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic path protection configuration Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection configuration protection switching occurred because of a PDI-P, page 2-126. The path protection configuration is configured for revertive switching and reverts 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 2-127.

**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).

## 2.6.22  AUTOSW-SDBER

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic path protection configuration Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade [SD, page 2-139] caused automatic path protection configuration protection switching to occur. The path protection configuration 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 2-140.

**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-SFBER

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal fail SF, page 2-141, caused automatic path protection configuration protection switching to occur. The path protection configuration 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 2-142.

**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 (STSMON)

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Automatic path protection configuration Switch Caused by Unequipped (UNEQ-P, page 2-159), indicates that an UNEQ alarm caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts 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 2-159.

**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).

## 2.6.25  AUTOSW-UNEQ (VTMON)

- Minor (MN), Service Affecting (SA)

AUTOSW-UNEQ (VTMON) indicates that an UNEQ-V alarm caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts 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 2-161.

**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).

## 2.6.26  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 15454. 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-A-LOW-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The Low Voltage Battery A 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 15454. 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).

## 2.6.28 BAT-B-HGH-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The High Voltage Battery B 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 15454. 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 BAT-B-LOW-VLT

- Not Reported (NR), Non-Service Affecting (NSA)

The Low Voltage Battery B 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 15454. 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).

# 2.6.30  BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)

The Primary Non-Volatile Backup Memory Failure alarm refers to a problem with the TCC+/TCC2 card's flash memory. The alarm occurs when the TCC+/TCC2 card is in use and has one of four problems: the flash manager fails to format a flash partition; the flash manager fails to write a file to a flash partition; there is a problem at the driver level, or the code volume fails cyclic redundancy checking (CRC). CRC is a method to verify for errors in data transmitted to the TCC+/TCC2.

The BKUPMEMP alarm can also cause an EQPT alarm. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

⚠
**Caution**    It can take up to 30 minutes for software to be updated on a standby TCC+/TCC2 card.

## Procedure:  Clear the BKUPMEMP Alarm

**Step 1**    Verify that both TCC+/TCC2 cards are powered and enabled by confirming lighted ACT/STBY LEDs on the TCC+/TCC2 cards.

**Step 2**    If both TCC+/TCC2 cards are powered and enabled, reset the active TCC+/TCC2 card to make the standby TCC+/TCC2 card active. Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 3**    If the TCC+/TCC2 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 TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

# 2.6.31  BLSROSYNC

- Major (MJ), Service Affecting (SA)

The BLSR Out Of Synchronization 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.

## 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

**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).

# 2.6.32  CARLOSS (EQPT)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN Equipment alarm occurs when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC+/TCC2 card or the LAN backplane pin connection on the ONS 15454. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the ONS 15454.

## Procedure:  Clear the CARLOSS (EQPT) Alarm

**Step 1**    Verify connectivity by pinging the ONS 15454 that is reporting the alarm:

**a.**    If you are using a Microsoft Windows operating system, from the Start Menu choose **Programs > Accessories > Command Prompt**.

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

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

**ping [ONS 15454 IP address]**

For example, ping 192.1.0.2.

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

**Step 2**    If the ping is successful, an active TCP/IP connection exists. Restart CTC:

**a.**    Exit from CTC.

**b.**    Reopen the browser.

**c.**    Log into CTC.

**Step 3**    Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

**Step 4**    If the straight-through (CAT-5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

**Step 5**    If you are unable to establish connectivity, 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 cables 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).

# 2.6.33  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), page 2-105. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet GBIC fiber connected to an optical (traffic) card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled (in service, IS) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes spanning tree protocol (STP). The database restoration circumstance applies to the E-series Ethernet cards but not the G1000-4 card, because the G1000-4 card does not use STP and is unaffected by STP reestablishment.

⚠️

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

## Procedure:  Clear the CARLOSS (E-Series) Alarm

Step 1  Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

Step 2  If the straight-through (CAT-5) LAN cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3  If no misconnection to an OC-N card exists, 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 (CAT-5) LAN cable connecting the transmitting device to the Ethernet port.

Step 6  If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the Ethernet (traffic) card.

Step 7  If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the Ethernet card.

⚠️

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

📝

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

**Step 8**   If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

**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 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

   • Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.

   • Double-click the Ethernet card that is part of the Ethernet manual cross-connect.

   • Click the **Circuits** tab.

   • Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

   **e.**   Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

   If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-167 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 10**   If the alarm does not clear, log 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  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), page 2-105. The Ethernet card has lost its link and is not receiving a valid signal.

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

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

- If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting G1000-4 card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as TPTFAIL (G-Series), page 2-156, or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G-Series) alarm.

Refer to the *Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" section on page 2-158 for more information about alarms that occur when a point-to-point circuit exists between two G1000-4 cards.

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

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

## Procedure:  Clear the CARLOSS (G-Series) Alarm

**Step 1**    Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

**Step 2**    If the straight-through (CAT-5) LAN cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

**Step 3**    If no misconnection to the OC-N card exists, 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 (CAT-5) LAN cable connecting the transmitting device to the Ethernet port.

**Step 6**    If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the G1000-4 card 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 G1000-4 card.

   **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) is also reported, complete the "Clear the TPTFAIL (G-Series) Alarm" procedure on page 2-157. 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 G1000-4's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

**Step 9**    If the TPTFAIL alarm was not reported, verify whether a terminal loopback has been provisioned on the port:

   **a.**    In the 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 IS is listed, go to Step 11.

**Step 10**    If a loopback was provisioned, complete the "Clear a Loopback" procedure on page 2-167.

On the G1000-4 card, provisioning a terminal loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 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 15454s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

   **a.**    Right-click anywhere 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 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

   - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.

   - Double-click the Ethernet (traffic) card that is part of the Ethernet manual cross-connect.

   - Click the **Circuits** tab.

   - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

   **e.**    Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

   **f.**    If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-167 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 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 2-170.

**Step 13** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the Ethernet card.

⚠️

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

✎

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

**Step 14** If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.35  CARLOSS (ML-Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the ML-series Ethernet (traffic) card is the data equivalent of an LOS (OC-N), page 2-105. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm is caused when the Ethernet port has been configured from the internal operating system (IOS) command line interface (CLI) as a no shutdown port and one of the following items also occurs:

- The cable is not properly connected to the near or far port
- Auto-negotiation is failing
- The speed (10/100 ports only) is set incorrectly

For information about provisioning ML-series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

### Procedure:  Clear the CARLOSS (ML-Series) Alarm

**Step 1** Verify that the LAN cable is properly connected and attached to the correct port on the ML-series card and on the peer Ethernet port.

**Step 2** If the alarm does not clear, verify that autonegotiation is set properly on the ML card port and the peer Ethernet port.

**Step 3** If the alarm does not clear, verify that the speed is set properly on the ML card port and the peer Ethernet port if you are using 10/100 ports.

**Step 4** If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

**Step 5** If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the IOS CLI. Autonegotiation will restart.

**Step 6**   If the alarm does not clear, perform a facility loopback on the ML card. Complete the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5.

**Step 7**   If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168.

**Step 8**   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169.

⚠

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

✎

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

**Step 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).

## 2.6.36  CKTDOWN

- Critical (CR), Service Affecting (SA)

The UCP Circuit Down alarm applies to logical circuits created within the UCP between devices. It occurs when the there is signaling failure across a UCP interface. The failure can be caused by a number of things, such as failure to route the call within the core network. In that case, the alarm cannot be resolved from the ONS 15454 because it is an edge device.

## Procedure:  Clear the CKTDOWN Alarm

**Step 1**   Ensure that the channel to neighbor has been provisioned with the correct IP address:

**a.**   In the node view, click the **Provisioning > UCP > Neighbor** tabs.

**b.**   View the entries to find out whether the node you are trying to contact is listed.

The node name is listed under the Name column and the IP address is listed under the Node ID column. If the Node ID says 0.0.0.0 and the Enable Discovery check box is selected, the node could not automatically identify the IP address. Ping the node to ensure that it is physically and logically accessible.

**c.**   Click **Start > Programs > Accessories > Command Prompt** to open an MS-DOS command window for pinging the neighbor.

**d.**   At the command prompt (C:\>), type:

```
ping [node DNS name or node IP address]
```

If you typed the domain name services (DNS) name and the ping was successful, you will see:

```
pinging [node dns name].[domain name].com. [node IP address] with 32 bytes of data:
Reply from [IP address]: bytes=32 time=10ms TTL=60
Reply from [IP address]: bytes=32 time=10ms TTL=60
```

```
Reply from [IP address]: bytes=32 time=10ms TTL=60
Reply from [IP address]: bytes=32 time=10ms TTL=60

Ping statistics for [IP address]:
Packets sent = 4 Received = 4 Lost = 0 (0% lost),
Approximate round trip time in milli-seconds:
Minimum = [minimum ms], Maximum = [maximum ms], Average = [average ms]
```

If you typed the IP address and the ping command is successful, the result will look similar but will not include the DNS name in the first line.

**e.** If your DNS name or IP address ping was successful, IP access to the node is confirmed, but your neighbor configuration is wrong. Delete the neighbor by selecting it in the window and clicking **Delete**.

**f.** If the ping was unsuccessful, you will get the following reply repeated for each try:

```
Request timed out.
```

A negative reply indicates that the neighbor node is not physically or logically accessible. Resolve the access problem, which is probably a cabling issue.

**Step 2** If the channel to neighbor has not been provisioned, or if you had to delete the channel, create one:

**a.** In the Provisioning > UCP > Neighbor tabs, click the **Create** button.

**b.** In the Neighbor Discovery window, enter the node's DNS node name in the Neighbor Name field. Leave the Enable Discovery check box checked (default setting) if you want the neighbor to be discovered through the network.

**c.** Click **OK**.

The node is listed in the Neighbor column list. If the neighbor discovery worked, the neighbor IP address is listed in the Node ID column. If it is not successful, the column will say 0.0.0.0.

**Step 3** If neighbor discovery is enabled, make sure that the neighbor node ID, remote IPCC have been discovered correctly.

**Step 4** Click the **Provisioning > UCP > IPCC** tabs and view the IPCC listing. If the IPCC has been created correctly, the Remote IP column contains the neighbor's IP address.

**Step 5** If the neighbor IP address is not correctly discovered, the field contains 0.0.0.0.

**a.** Click the entry to select the neighbor IP address and click **Delete**.

**b.** If you get an error that will not allow you to delete the IPCC, you will have to delete the neighbor and recreate it. Click the **Neighbor** tab.

**c.** Click to select the neighbor and click **Delete**.

**d.** Then go back to Step 2 to recreate the neighbor.

**Step 6** If remote IPCC has not been discovered, or if it had to be deleted, create the connection:

**a.** In the Provisioning > UCP > IPCC tabs, click **Create**.

**b.** In the Unified Control Plane Provisioning window, click **Next**.

**c.** If no IPCCs are listed, click **Create**.

**d.** In the Create New IPCC window, click one of the DCC terminations in the DCC list.

Leave the SDCC radio button selected (as long as DCCs have been created on the node) and leave the Leave Unchanged radio button selected.

**e.** Click **OK**. The IPCC is listed as CCID 1 in the Unified Control Plane Provisioning window.

**f.** Click the neighbor to select it, and click **Next**.

**g.** Choose a UCP interface (for example Slot 5 (OC48), port 1) from the pull-down menu. The field default is the node where you are logged in.

**h.** Choose the UCP interface TNA address type. The default is IPv4. The address field lists the login node IP address by default.

**i.** Click **Finish**. If creation is successful, the Remote ID column in the IPCC tab will contain the neighbor's IP address.

**Step 7** Ensure that the local and remote interface IDs have been provisioned correctly:

**a.** Click the **Interface** tab. View the slot and port listed in the Interface column (for example, Slot 5 (OC48), port 1).

**b.** Compare the listed interface listed with the IPCC tab **SDCC** column entry.

**Step 8** If the Interface column is not the same as the SDCC column entry, click the entry in the Interface window to select it and click **Delete**.

**Step 9** Click **Next**.

**Step 10** In the Existing CCIDs list, click the IPCC containing the DCC connection. Click **Next**.

The correct interface for the selected CCID is shown in the UPC Interface field, and the correct IP address information for the login node is shown by default in the other fields. Click **Finish**.

**Step 11** If you completed all of these steps and verified the information, the alarm could be the result of a misconfiguration in the core network. Contact the core site administrators.

**Step 12** If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.37  CLDRESTART

- Not Alarmed (NA), (Non-Service Affecting (NSA)

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 is first powered up.

⚠️

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

## Procedure:  Clear the CLDRESTART Condition

**Step 1** If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168.

**Step 2** If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the card.

⚠

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

✎

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

**Step 3**   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.38  COMIOXC

- Critical (CR), Service Affecting (SA)

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the cross-connect card. It occurs when there is a communication failure for a traffic (multispeed slots or high-speed) slot.

### Procedure:  Clear the COMIOXC Alarm

**Step 1**   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 on the reporting cross-connect 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 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

**Step 3**   If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-166.

**Step 4**   Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting cross-connect card.

**Step 5**   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting cross-connect card.

✎

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

**Step 6**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.39  CONTBUS-A-18

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

A Communication Failure from TCC+/TCC2 Slot to TCC+/TCC2 Slot alarm occurs when the main processor on the TCC+/TCC2 card in Slot 7 (termed TCC A) loses communication with the coprocessor on the same card.

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

### Clear the CONTBUS-A-18 Alarm

**Step 1**    Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the TCC+/TCC2 in Slot 11 active.

**Step 2**    Wait approximately 10 minutes for the TCC+/TCC2 in Slot 7 to reset as the standby TCC+/TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

**Step 3**    Position the cursor over the TCC+/TCC2 card in Slot 11 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the standby TCC+/TCC2 in Slot 7 active.

**Step 4**    If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

## 2.6.40  CONTBUS-B-18

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

A Communication Failure from TCC+/TCC2 Slot to TCC+/TCC2 Slot alarm occurs when the main processor on the TCC+/TCC2 card in Slot 11 (termed TCC B) loses communication with the coprocessor on the same card.

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

## Clear the CONTBUS-B-18 Alarm

**Step 1**   Position the cursor over the TCC+/TCC2 card in Slot 11 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the TCC+/TCC2 in Slot 7 active.

**Step 2**   Wait approximately 10 minutes for the TCC+/TCC2 in Slot 11 to reset as the standby TCC+/TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

**Step 3**   Position the cursor over the TCC+/TCC2 card in Slot 7 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the standby TCC+/TCC2 in Slot 11 active.

**Step 4**   If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

# 2.6.41  CONTBUS-IO-A

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

A TCC A to Shelf Slot Communication Failure alarm occurs when the active TCC+/TCC2 card in Slot 7 (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm might appear briefly when the ONS 15454 switches to the protect TCC+/TCC2 card. In the case of a TCC+/TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC+/TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC+/TCC2 card to the reporting card. The physical path of communication includes the TCC+/TCC2 card, the other card, and the backplane.

This alarm can also appear when you upgrade from TCC+ cards to TCC2 cards. In this case, it clears without intervention within about 13 minutes.

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

## Clear the CONTBUS-IO-A Alarm

**Step 1**   Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the MEA (BP) alarm (see page 2-114) for the reporting card.

**Step 2**   If the alarm object is any single card slot other than the standby TCC+/TCC2 in Slot 11, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169. Verify that the following LED behavior takes place:

 • 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 3**    If the alarm object is the standby TCC+/TCC2 in Slot 11, perform a soft reset of this card:

    **a.**    Right-click the Slot 11 TCC+/TCC2 card.

    **b.**    Choose **Reset Card** from the shortcut menu.

    **c.**    Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 4**    If CONTBUS-IO-A is raised on several cards at once, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 5**    Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify that the SBY LED is blinking on the standby card.

**Step 6**    If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting card.

**Step 7**    If the reseated card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

# 2.6.42  CONTBUS-IO-B

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

A TCC B to Shelf Slot Communication Failure alarm occurs when the active TCC+/TCC2 card in Slot 11 (TCC B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm might appear briefly when the ONS 15454 switches to the protect TCC+/TCC2 card. In the case of a TCC+/TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC+/TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC+/TCC2 card to the reporting card. The physical path of communication includes the TCC+/TCC2 card, the other card, and the backplane.

This alarm can also appear when you upgrade from TCC+ cards to TCC2 cards. In this case, it clears without intervention within about 13 minutes.

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

## Clear the CONTBUS-IO-B Alarm

**Step 1**    Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the MEA (BP) alarm (see page 2-114) for the reporting card.

**Step 2** If the alarm object is any single card slot other than the standby TCC+/TCC2 in Slot 7, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169. Verify that the following LED behavior takes place:

- 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 3** If the alarm object is the standby TCC+/TCC2 in Slot 7, perform a soft reset of this card:

**a.** Right-click the Slot 7 TCC+/TCC2 card.

**b.** Choose **Reset Card** from the shortcut menu.

**c.** Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 4** If CONTBUS-IO-B is raised on several cards at once, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 5** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify that the SBY LED is blinking on the standby card.

**Step 6** If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting card.

**Step 7** If the reseated card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

## 2.6.43 CTNEQPT-PBPROT

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the Slot 10 cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card, the reporting traffic card, the TCC+/TCC2 card, or the backplane.

**Note** If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the standby TCC+/TCC2 card. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-169 for the standby TCC+/TCC2 card. Do not physically reseat an active TCC+/TCC2 card. Reseating the TCC+/TCC2 disrupts traffic.

**Note** This alarm is automatically raised and then cleared when the Slot 8 XC card is reseated.

**Caution** It can take up to 30 minutes for software to be updated on a standby TCC+/TCC2 card.

⚠

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

## Procedure:  Clear the CTNEQPT-PBPROT Alarm

**Step 1**    Perform a CTC reset on the standby cross-connect card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169.

- 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 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

If the cross-connect reset is not complete and error-free or if the TCC+/TCC2 reboots automatically, call TAC (1-800-553-2447).

**Step 3**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the standby cross-connect card.

**Step 4**    Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status will be displayed in the list.

**Step 5**    If the reporting traffic card is the active card in the protection group, complete the "Switch Protection Group Traffic with an External Switching Command" procedure on page 2-166. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

**Step 6**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 on 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 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

**Step 8**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

**Step 9**    Complete the "Clear an External Switching Command" procedure on page 2-167.

**Step 10**    If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting traffic card.

⚠️

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

**Step 11**    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).

## 2.6.44 CTNEQPT-PBWORK

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the Slot 8 cross-connect card the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card, the reporting traffic card, or the backplane.

✎

**Note**    If all traffic cards show CTNEEQPT-PBWORK alarm, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 for the active TCC+/TCC2 card and then complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-169 for the TCC+/TCC2 card. Do not physically reseat an active TCC+/TCC2 card; it disrupts traffic.

✎

**Note**    This alarm is automatically raised and then cleared when the Slot 10 XC card is reseated.

⚠️

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

## Procedure:  Clear the CTNEQPT-PBWORK Alarm

**Step 1**    Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-166 for the active cross-connect card.

✎

**Note**    After the active cross-connect goes into standby, the original standby slot becomes active. The active card ACT/STBY LED becomes green.

**Step 2**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 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 15454, the ACT/STBY LED is illuminated.

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

**Step 4**  If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the standby cross-connect card.

**Note**  The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is 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 2-166. 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 2-169 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 15454, the ACT/STBY LED is illuminated.

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

**Step 8**  If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

**Step 9**  If you switched traffic, complete the "Clear an External Switching Command" procedure on page 2-167.

**Step 10**  If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the cross-connect card.

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

**Step 11**  If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting traffic card.

**Step 12**  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).

## 2.6.45 DATAFLT

- Minor (MN), Non-Service Affecting (NSA)

The Software Data Integrity Fault alarm occurs when the TCC+/TCC2 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 Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

**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  DBOSYNC

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

The standby Database Out Of Synchronization alarm occurs when the standby TCC+/TCC2 "To be Active" database does not synchronize with the active database on the active TCC+/TCC2.

⚠

**Caution**    If you reset the active TCC+/TCC2 card while this alarm is raised, you will lose current provisioning.

## Procedure: Clear the DBOSYNC Alarm

**Step 1**    Save a backup copy of the active TCC+/TCC2 database. Complete the "Back Up the Database" procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 2**    Make a minor provisioning change to the active database to see if applying a provisioning change if applying a provisioning change clears the alarm:

**a.**    In the 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 will 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).

## 2.6.47  DS3-MISM

- Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-3 Frame Format Mismatch condition indicates a frame format mismatch on a signal transiting the DS3XM-6 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type is set to C-BIT for a DS3XM-6 card, and the incoming signal's frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

### Procedure:  Clear the DS3-MISM Condition

**Step 1**    Display the CTC card view for the reporting DS3XM-6 card.

**Step 2**    Click the **Provisioning > Line** tabs.

**Step 3**    For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal.

**Step 4**    If the Line Type pull-down menu does not match the expected incoming signal, select the correct Line Type in the pull-down menu.

**Step 5**    Click **Apply**.

**Step 6**    If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal.

For specific procedures to use the test set equipment, consult the manufacturer.

**Step 7**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.48  DSP-COMM-FAIL

- Major (MJ), Service Affecting (SA)

The DSP Communication Failure alarm indicates that there is a communications failure between a muxponder (MXP) or transponder (TXP) card microprocessor and the on-board DSP chip that controls the trunk (DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP or TXP card microprocessor will attempt to restore communication with the DSP chip until the alarm is cleared.

If the alarm remains for an extended period, The MXP or TXP card will raise DSP-FAIL, page 2-55.

**Note**    If the DSP-COMM-FAIL alarm continues for an extended period, traffic could be affected.

**Note**    DSP-COMM-FAIL is informational. The alarm does not require troubleshooting.

## 2.6.49  DSP-FAIL

- Major (MJ), Service Affecting (SA)

The DSP Failure alarm indicates that a DSP-COMM-FAIL, page 2-55, has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

### Procedure:  Clear the DSP-FAIL Alarm

**Step 1**    Complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

⚠️

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

**Step 2**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.50  EHIBATVG-A

- Minor (MN), Non-Service Affecting (NSA)

The Extreme High Voltage Battery A alarm occurs when the voltage level on battery lead A exceeds –56.7 VDC. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains 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 15454. 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).

## 2.6.51  EHIBATVG-B

- Minor (MN), Non-Service Affecting (NSA)

The Extreme High Voltage Battery B alarm occurs when the voltage level on battery lead B exceeds –56.7 VDC. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains 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 15454. 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).

## 2.6.52  ELWBATVG-A

- Minor (MN), Non-Service Affecting (NSA)

The Extreme Low Voltage Battery A alarm occurs when the voltage on battery feed A is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery A alarm occurs when the voltage on battery feed A 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 15454. 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).

# 2.6.53  ELWBATVG-B

- Minor (MN), Non-Service Affecting (NSA)

The Extreme Low Voltage Battery B alarm occurs when the voltage on battery feed B is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery B alarm occurs when the voltage on battery feed B 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 15454. 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).

# 2.6.54  EOC

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

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

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

**Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

**Note**    If a circuit shows an incomplete state when the EOC alarm is raised, it occurs when the logical circuit is in place, 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 is also reported complete the "Clear the LOS (DS-1) Alarm" procedure on page 2-101.

**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 2-165 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 IS.

    **e.**    If the State column lists the port as OOS, click the column and click **IS** from the pull-down menu. Click **Apply**.

**Step 7**    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 card. It might be necessary to manually switch traffic carrying circuits over to a protection path.

**Step 8**    If no signal failures on terminations exist, measure power levels to verify that the budget loss is within the parameters of the receiver. See the "Optical Card Transmit and Receive Levels" section on page 1-84.

**Step 9**    If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the "Install the Fiber-Optic Cables" procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 10**    If fiber connectors are properly fastened and terminated, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC+/TCC2 switches control to the standby TCC+/TCC2. If the alarm clears when the ONS 15454 switches to the standby TCC+/TCC2, the user can assume that the original active TCC+/TCC2 is the cause of the alarm.

**Step 11**    If the TCC+/TCC2 replacement does not clear the alarm, delete the problematic DCC termination:

**a.**    Click the **Provisioning > DCC/GCC** 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 15454 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 TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

## 2.6.55  EQPT

- Critical (CR), Service Affecting (SA)

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

If the EQPT alarm occurs with a BKUPMEMP alarm, see the "BKUPMEMP" section on page 2-36. The BKUPMEMP procedure also clears the EQPT alarm.

⚠

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

### Procedure:  Clear the EQPT Alarm

**Step 1**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 15454, the ACT/STBY LED is illuminated.

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

**Step 3**    If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting card.

**Step 4**    If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

✎

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

**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).

## 2.6.56  EQPT-MISS

- Critical (CR), Service Affecting (SA)

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

⚠

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

### Procedure:  Clear the EQPT-MISS Alarm

**Step 1**    If the alarm is reported against the fan, 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 2-170.

**Step 3**    If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the "Install the Fan-Tray Assembly," procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 4**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.57  ERROR-CONFIG

- Minor (MN), Non-Service Affecting (NSA)

The Error in Startup Configuration alarm applies to the ML-series Ethernet (traffic) cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are that (1) you stored the configuration for one type of ML card in the database and then installed another type in its slot, and (2) the configuration file contained a syntax error on one of the lines.

For information about provisioning the ML-series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

## Procedure:  Clear the ERROR-CONFIG Alarm

**Step 1**    If you have a different type of ML card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

**Step 2**    Upload the configuration file to the TCC+/TCC2:

   **a.**  In the node view, right-click the ML card graphic.

   **b.**  Choose **IOS Startup Config** from the shortcut menu.

   **c.**  Click **Upload to TCC** and navigate to the file location.

**Step 3**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169.

**Step 4**    If the alarm does not clear or if your configuration file was correct according to the installed card, start an IOS CLI for the card:

   **a.**  Right click the ML card graphic in node view.

   **b.**  Choose **Open IOS Connection** from the shortcut menu.

   > ✎
   > **Note**    Open IOS Connection is not available unless the ML card is physically installed in the shelf.

   Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* to correct the errored configuration file line.

**Step 5**    Execute the CLI command **copy run start**. The command copies the new card configuration into the database and clears the alarm.

**Step 6**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.58  E-W-MISMATCH

   •  Major (MJ), Service Affecting (SA)

A Procedural Error Misconnect East/West Direction 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.

Note    The E-W-MISMATCH alarm also appears during the initial set up of a ring with its East-West slots configured correctly. If the alarm appears during the initial setup, the alarm clears itself shortly after the ring setup is complete.

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

Note    The physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slots as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

## 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 the node view, click **View > Go to Network View**.

Step 3    Label each of the nodes on the diagram with the same name that appears on the network map.

Step 4    Right-click each span to reveal the node name/slot/port for each end of the span.

Step 5    Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 - Node2/Slot6/Port1 (2F BLSR OC48, Ring 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.

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

Warning    **Invisible laser radiation 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.**

**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 2-164 to identify the node ID, ring ID, and the slot and port in the East Line list and West Line columns. Record the above information.

**Step 4**   Click **View > Go to Network View**.

**Step 5**   Delete and recreate the BLSR:

    **a.**   Click the **Provisioning > BLSR** tabs.

    **b.**   Click the row from Step 3 to select it and click **Delete**.

    **c.**   Click **Create**.

    **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 pull-down menu to the slot you recorded for the East Line in Step 3.

**Step 8**   Change the East Line pull-down menu to the slot you recorded for the West Line in Step 3.

**Step 9**   Click **OK**.

**Step 10**   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.59  EXCCOL

- Minor (MN), Non-Service Affecting (NSA)

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 and CTC might be affected.The network management LAN is the data network connecting the workstation running the CTC software to the TCC+/TCC2 card. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC+/TCC2 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 TCC+/TCC2 card has a flow rate set to 10 Mb, half-duplex.

**Step 2**  If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC+/TCC2 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).

## 2.6.60  EXERCISE-RING-REQ

• Not Alarmed (NA), Non-Service Affecting (NSA)

The Exercise Request on Ring condition occurs when optical (traffic) cards in two-fiber and four-fiber BLSRs are tested using the EXERCISE RING command.

**Note**  EXERCISE-RING-REQ is an informational condition. It does not require troubleshooting.

## 2.6.61  EXERCISE-SPAN-REQ

• Not Alarmed (NA), Non-Service Affecting (NSA)

The Exercise Request on Span condition occurs when optical (traffic) cards in a four-fiber BLSR are tested using the EXERCISE SPAN command.

**Note**  EXERCISE-SPAN-REQ is an informational condition. It does not require troubleshooting.

## 2.6.62  EXT

• Minor (MN), Non-Service Affecting (NSA)

A Failure Detected External to the NE 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 the node view, double-click the AIC or AIC-I card to display the card view.

**Step 2**  Click the **Maintenance** tab to gather further information about the EXT alarm.

**Step 3**  Perform your standard operating procedure for the environmental condition.

**Step 4**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.63 EXTRA-TRAF-PREEMPT

- Major (MJ), Service Affecting (NSA)

An Extra Traffic Preempted alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

### 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 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).

## 2.6.64 FAILTOSW

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Failure to Switch to Protection condition occurs when a working electrical (traffic) card cannot switch to the protect card in a 1:N protection group, because another working electrical (traffic) card with a higher-priority alarm has switched to the protect card.

### Procedure:  Clear the FAILTOSW Condition

**Step 1**    Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the 1:N card and clears the FAILTOSW.

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

**Step 2**    If the condition does not clear, replace the working electrical (traffic) card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 2-169. This card is the working electrical card using the 1:N card protection and not reporting FAILTOSW.

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

Replacing the working electrical card 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.

&#9998;

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

**Step 3**     If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.65 FAILTOSW-PATH

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Fail to Switch to Protection Path condition occurs when the working path does not switch to the protection path on a path protection configuration. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection card or a lock out set on one of the path protection configuration nodes.

&#9888;

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

## Procedure:  Clear the FAILTOSW-PATH Condition in a Path Protection Configuration Configuration

**Step 1**     Look up and clear the higher priority alarm. Clearing this condition frees the standby card and clears the FAILTOSW-PATH condition.

**Step 2**     If the condition does not clear, replace the active OC-N card that is reporting the higher priority alarm. Complete the "Physically Replace a Card" procedure on page 2-169. Replacing the active OC-N card that is reporting the higher priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower priority alarm and the FAILTOSW-PATH condition.

&#9888;

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

&#9998;

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

**Step 3**     If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.66 FAILTOSWR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Fail to Switch to Protection Ring condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears when one of the following 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, page 2-139, or an SF, page 2-141] clears.

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

⚠ **Warning**  **Invisible laser radiation 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 FAILTOSWR Condition in a Four-Fiber 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 pull-down menu.

**Step 2**  If the condition does not clear, in the 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 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 OK, verify that the correct port is in service:

  **a.**  Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

**b.** To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

**c.** Click the **Provisioning > Line** tabs.

**d.** Verify that the **State** column lists the port as IS.

**e.** If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 8** If the correct port is in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

⚠ **Caution** Using an optical test set disrupts service on the optical (traffic) card. It 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 15454 Procedure Guide*.

**Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-84 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 2-169 for the protect standby OC-N card.

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

**Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4–12 for each of the nodes in the ring.

**Step 14** If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.67  FAILTOSWS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following actions occur: a higher priority event, such as an external switch command occurs, the next span switch succeeds, or the cause of the APS switch [such as SD, page 2-139, or SF, page 2-141] clears.

# 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 pull-down menu.

**Step 2**    If the condition does not clear, in the 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:

   **a.**    Confirm that the OC-N card shows a green LED in CTC or on the physical card.

      A green LED indicates an active card. An amber LED indicates a standby card.

   **b.**    To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

   **c.**    Click the **Provisioning > Line** tabs.

   **d.**    Verify that the **State** column lists the port as IS.

   **e.**    If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 6**    If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.

**Step 7**    If fiber continuity to the ports is OK, verify that the correct port is in service:

   **a.**    Confirm that the OC-N card shows a green LED in CTC or on the physical card.

      A green LED indicates an active card. An amber LED indicates a standby card.

   **b.**    To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

   **c.**    Click the **Provisioning > Line** tabs.

   **d.**    Verify that the **State** column lists the port as IS.

   **e.**    If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 8**    If the correct port is in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

⚠ **Caution**    Using an optical test set disrupts service on the optical (traffic) card. It 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 15454 Procedure Guide*.

**Step 10**    If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-84 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 2-169 for the protect standby OC-N card.

⚠

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

**Step 13**    If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4–12 for each of the nodes in the ring.

**Step 14**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.68  FAN

- Critical (CR), Service Affecting (SA)

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

⚠

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

## Procedure:  Clear the FAN Alarm

**Step 1**    Verify whether the air filter to see whether it needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 3-5.

**Step 2**    If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-170.

✎

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

**Step 3**    If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

**Step 4**    If the replacement fan-tray 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).

## 2.6.69  FANDEGRADE

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

The Partial Fan Failure Speed Control Degradation 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 2-70.

**Step 2**      If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (TAC) at 1-800-553-2447.

## 2.6.70  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), page 2-105, downstream.

### Procedure:  Clear the FE-AIS Condition

**Step 1**      Complete the "Clear the AIS Condition" procedure on page 2-21.

**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).

## 2.6.71  FE-DS1-MULTLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Multiple DS-1 LOS Detected condition occurs when multiple DS-1 signals are lost on a far-end DS-1 card. The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. 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. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2**      Log into the node that links directly to the card reporting the FE condition.

**Step 3**      Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.72  FE-DS1-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-1 Equipment Failure Non-Service Affecting condition occurs when a far-end DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

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

**Step 1**    To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 might link to an alarm from a card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.73  FE-DS1-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-1 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on a DS-1 card that affects service because traffic is unable to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

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

**Step 1**    To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 might link to an alarm from a card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**   Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.74  FE-DS1-SNGLLOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment. Signal loss also causes an LOS (OC-N), page 2-105. The prefix FE in an alarm or condition means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-SNGLLOS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. 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 link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 might link to an alarm from a card in Slot 6 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**   Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.75  FE-DS3-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-3 Equipment Failure Non-Service Affecting condition occurs when a far-end DS-3 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

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

**Step 1**   To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 might link to an alarm from a card in Slot 6 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.76  FE-DS3-SA

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End DS-3 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on a DS-3 card that affects service because traffic is unable to switch to the protect port.

The prefix FE in an alarm or condition means the main alarm is occurring at the far-end node and not at the node reporting the FE condition. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. 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 link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 might link to an alarm from a card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.77  FE-EQPT-NSA

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

⚠

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

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

**Step 1**    To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

**Step 4**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.78  FE-EXERCISING-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Exercising Ring condition occurs when far-end optical (traffic) cards in a two-fiber or four-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.

# 2.6.79  FE-EXERCISING-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Exercising Span condition occurs when far-end optical (traffic) cards in a four-fiber 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.

# 2.6.80  FE-FRCDWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Ring Working Facility Forced to Switch to Protection 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.

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

## Procedure:  Clear the FE-FRCDWKSWPR-RING Condition

**Step 1**   To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 might link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**   Clear the main alarm. See the "Clear a BLSR Span Lock Out" procedure on page 2-165 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).

# 2.6.81  FE-FRCDWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the FORCE SPAN command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

## Procedure:  Clear the FE-FRCDWKSWPR-SPAN Condition

**Step 1**   To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 might link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**   Clear the main alarm. See the "Clear a BLSR Span Lock Out" procedure on page 2-165 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).

# 2.6.82  FE-IDLE

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Idle condition occurs when a far-end node detects an idle DS-3 signal.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-IDLE condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

## Procedure:  Clear the FE-IDLE Condition

**Step 1**    To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Clear the main alarm. Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

**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).

# 2.6.83  FE-LOCKOUTOFPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End lock out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a far-end node using the LOCKOUT 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 link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 might link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

**Step 2**    Log into the node that links directly to the card reporting the FE condition.

**Step 3**    Make sure there is no lock out set. See the "Clear a BLSR Span Lock Out" procedure on page 2-165 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).

# 2.6.84  FE-LOF

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End LOF condition occurs when a far-end node reports an LOF (DS-3), page 2-95.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end node and not at the node reporting the FE-LOF condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Chapter 2      Alarm Troubleshooting

**Alarm Procedures**

## Procedure: Clear the FE-LOF Condition

**Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2** Log into the node that links directly to the card reporting the FE condition.

**Step 3** Complete the "Clear the LOF (DS-1) Alarm" procedure on page 2-94. It 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).

## 2.6.85  FE-LOS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End LOS condition occurs when a far-end node reports an LOS (DS-3), page 2-102.

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 link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2** Log into the node that links directly to the card reporting the FE condition.

**Step 3** Complete the "Clear the LOS (DS-1) Alarm" procedure on page 2-101.

**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).

## 2.6.86  FE-MANWKSWPR-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when a BLSR working ring is switched from working to protect at a far-end node using the MANUAL RING command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-MANWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

**2-78**

July 2005

## Procedure: Clear the FE-MANWKSWPR-RING Condition

**Step 1**  To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 might link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

**Step 2**  Log into the node that links directly to the card reporting the FE condition.

**Step 3**  Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

**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).

# 2.6.87  FE-MANWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Far-End Manual Switch Span Working Facility to Protect 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 link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 might link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

**Step 2**  Log into the node that links directly to the card reporting the FE condition.

**Step 3**  Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

**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).

# 2.6.88  FEPRLF

- Minor (MN), Non-Service Affecting (NSA)

The Far End Protection Line Failure alarm occurs when an APS channel SF, page 2-141, occurs on the protect card coming into the node.

**Note**  The FEPRLF alarm occurs only on the ONS 15454 when bidirectional protection is used on optical (traffic) cards in a 1+1 configuration or 4-fiber BLSR configuration.

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

**Step 1**   To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE condition on a card in Slot 12 of Node 1 might relate to a main alarm from a card in Slot 6 of Node 2.

**Step 2**   Log into the node that links directly to the card reporting the FE condition.

**Step 3**   Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for instructions.

**Step 4**   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.89  FORCED-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

## Procedure:  Clear the FORCED-REQ Condition

**Step 1**   Complete the .

**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).

# 2.6.90  FORCED-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch Request Ring condition applies to optical trunk cards when the FORCE RING command is applied to two-fiber and four-fiber BLSRs to move traffic from working to protect.

## Procedure:  Clear the FORCED-REQ-RING Condition

**Step 1**   Complete the .

**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).

## 2.6.91  FORCED-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch Request Span condition applies to optical trunk cards in four-fiber BLSRs when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

### Procedure:  Clear the FORCED-REQ-SPAN Condition

**Step 1**    Complete the "Clear the FORCED-REQ Condition" 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 (1-800-553-2447).

## 2.6.92  FRCDSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.

**Note**    FRCDSWTOINT is an informational condition. It does not require troubleshooting.

## 2.6.93  FRCDSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.

**Note**    FRCDSWTOPRI is an informational condition. It does not require troubleshooting.

## 2.6.94  FRCDSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.

**Note**    FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

## 2.6.95 FRCDSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to the third timing source.

✎
**Note**     FRCDSWTOTHIRD is an informational condition. It does not require troubleshooting.

## 2.6.96 FRNGSYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

### Procedure:  Clear the FRNGSYNC Alarm

**Step 1**     If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC alarm.

**Step 2**     If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards.

**Step 3**     If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI, page 2-153, and SYNCSEC, page 2-154.

**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).

## 2.6.97 FSTSYNC

- Minor (MN), Non-Service Affecting (NSA)

A Fast Start Synchronization mode alarm occurs when the ONS 15454 is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

✎
**Note**     FSTSYNC is an informational alarm. It does not require troubleshooting.

## 2.6.98 FULLPASSTHR-BI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Bidirectional Full Pass-Through Active condition occurs on a non-switching 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 2-165.

**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  GCC-EOC

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

The GCC Embedded Operation Channel Failure alarm applies to the OTN communication channel for TXP and MXP cards. The GCC-EOC is raised when the channel cannot operate.

## Procedure:  Clear the GCC-EOC Alarm

**Step 1**    Complete the "Clear the EOC Alarm" procedure on page 2-58.

**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).

# 2.6.100  HI-LASERBIAS

- Minor (MN), Non-Service Affecting (NSA)

The Equipment High Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30% of the manufacturer's maximum laser bias specification and increases as the laser ages. So if the HI-LASERBIAS alarm threshold is set at 100% of the maximum, the laser's usability has ended. If the threshold is set at 90% of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

## Procedure:  Clear the HI-LASERBIAS Alarm

**Step 1**    Complete the "Clear the LASEREOL Alarm" procedure on page 2-91. Replacement is not urgent and can be scheduled during a maintenance window.

**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).

# 2.6.101 HI-LASERTEMP

- Minor (MN), Non-Service Affecting (NSA)

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card default level by 2° C.

**Note**    To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

## Procedure:  Clear the HI-LASERTEMP Alarm

**Step 1**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting MXP or TXP card.

**Step 2**    If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

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

**Step 3**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC at 1-800-553-2447.

# 2.6.102 HI-RXPOWER

- Minor (MN), Non-Service Affecting (NSA)

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP or MXP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

## Procedure:  Clear the HI-RXPOWER Alarm

**Step 1**    Find out whether gain (the amplification power) of any amplifiers has been changed. The change will also cause channel power to need adjustment.

**Step 2**    Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped off, the power levels of all channels will have to be adjusted.

**Note**    If the card is part of an amplified dense wavelength multiplexing system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

**Step 3**    At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

**Step 4**    If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at once and data alarms would be present. If wavelengths are drifting, the data will be garbled and receive power will increase by about +3dB.

**Step 5**    If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance according to standard practice.

**Step 6**    If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, use known-good loopback cable to complete the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5.

**Step 7**    If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Card" procedure on page 2-169. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

⚠

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

**Step 8**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.103  HI-RXTEMP

- Minor (MN) Non-Service Affecting (NSA)

The Equipment High Receive temperature alarm refers to the temperature of the trunk card port for the TXP and MXP cards. The HI-RXTEMP threshold is user-provisionable.

## Procedure:  Clear the HI-RXTEMP Alarm

**Step 1**    If an EXT alarm is also present, complete the "Clear the EXT Alarm" procedure on page 2-64.

**Step 2**    If a shelf HITEMP alarm is also present, complete the "Clear the HITEMP Alarm" procedure on page 2-86.

**Step 3**    If a HI-LASERTEMP alarm is also present, complete the "Clear the HI-LASERTEMP Alarm" procedure on page 2-84.

✎

**Note**    If no data alarms have occurred, the card does not need to be replaced immediately.

**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).

# 2.6.104 HITEMP

- Critical (CR), Service Affecting (SA) for NE

- Minor (MN), Non-Service Affecting (NSA) for EQPT

The High Temperature alarm occurs when the temperature of the ONS 15454 is above 122° F (50° C).

⚠

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

## Procedure:  Clear the HITEMP Alarm

**Step 1**    View the temperature displayed on the ONS 15454 LCD front panel. For an illustration of the LCD panel, refer to NTP-70, "View Alarm Counts on the LCD for a Slot or Port," in the *Cisco ONS 15454 Procedure Guide*.

**Step 2**    Verify whether the environmental temperature of the room is not abnormally high.

**Step 3**    If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454.

**Step 4**    If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 empty slots. Blank faceplates help airflow.

**Step 5**    If faceplates fill the empty slots, verify whether the air filter to see whether it needs replacement. Refer to NTP-107, "Inspect and Maintain the Air Filter," in the *Cisco ONS 15454 Procedure Guide*

**Step 6**    If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-170.

✎

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

**Step 7**    If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

**Step 8**    If the replacement fan-tray 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 it applies to the NE, or a non-service-affecting problem if it applies to equipment.

# 2.6.105 HI-TXPOWER

- Minor (MN), Non-Service Affecting (NSA)

The Equipment High Transmit Power alarm is an indicator on the TXP card and MXP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

## Procedure:  Clear the HI-TXPOWER Alarm

**Step 1**    In the node view, display the card view for the TXP or MXP card.

**Step 2**    Click the **Provisioning > Optical Thresholds** tabs.

**Step 3**    Decrease (i.e. change toward the negative direction) the TX Power High column value by 0.5 dBm.

**Step 4**    If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Card" procedure on page 2-169.

⚠️

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

**Step 5**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.106  HLDOVRSYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

## Procedure:  Clear the HLDOVRSYNC Alarm

**Step 1**    Clear additional alarms that relate to timing, such as FRNGSYNC, page 2-82; FSTSYNC, page 2-82; HLDOVRSYNC, page 2-87; LOS (BITS), page 2-101; LOS (BITS), page 2-101; MANSWTOINT, page 2-112; MANSWTOPRI, page 2-112; MANSWTOSEC, page 2-113; MANSWTOTHIRD, page 2-113; SWTOPRI, page 2-152; SWTOSEC, page 2-152; SWTOTHIRD, page 2-152; SYNC-FREQ, page 2-153; SYNCPRI, page 2-153; SYNCSEC, page 2-154, or SYNCTHIRD, page 2-154.

**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).

# 2.6.107  IMPROPRMVL

- Critical (CR), Service Affecting (SA)

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

⚠️

**Caution**    It can take up to 30 minutes for software to be updated on a standby TCC+/TCC2 card.

⚠️

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

⚠️

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

✎

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

## Procedure:  Clear the IMPROPRMVL Alarm

**Step 1**    In the 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 (OOS):

⚠️

**Caution**    Before taking a port out of service (OOS), ensure that no live traffic is present.

**a.**    In node view, double-click the reporting card to display the card view.

**b.**    Click the **Provisioning** tab.

**c.**    Click the **State** column of any in-service (IS) ports.

**d.**    Choose **OOS** to take the ports out of service.

**Step 4**    If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-167.

⚠️

**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 > DCC/GCC** tabs.

   **b.**    Click the slots and ports listed in DCC terminations.

   **c.**    Click **Delete** and click **Yes** in the dialog box that appears.

**Step 7**    If the card is used as a timing reference, change the timing reference:

   **a.**    Click the **Provisioning > Timing** tabs.

   **b.**    Under NE Reference, click the pull-down menu for **Ref-1**.

   **c.**    Change Ref-1 from the listed OC-N card to Internal Clock.

   **d.**    Click **Apply**.

**Step 8**    Right-click the card reporting the IMPROPRMVL alarm and choose **Delete**.

**Step 9**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.108  INC-ISD

   • Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an 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.

# 2.6.109  INHSWPR

   • Not Alarmed (NA), Non-Service Affecting (NSA)

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a1:N protection scheme, traffic can be switched between working cards when the switched to protect is disabled.

## Procedure:  Clear the INHSWPR Condition

**Step 1**    Complete the .

**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).

# 2.6.110 INHSWWKG

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a1:N protection scheme, traffic can be switched between protect cards when the switched to working is disabled.

## Procedure:  Clear the INHSWWKG Condition

**Step 1**    Complete the "Clear an External Switching Command" procedure on page 2-167.

**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).

# 2.6.111 INVMACADR

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

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

# 2.6.112 KB-PASSTHR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The K Bytes Pass Through Active 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 2-165.

**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).

# 2.6.113 LAN-POL-REV

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lan Connection Polarity Reversed condition is raised by the TCC+ card when the card detects that a connected Ethernet cable has reversed receive wire pairs. The TCC+ automatically compensates for this reversal, but LAN-POL-REV stays active. This condition usually occurs during software upgrades to Release 4.0 or in new NE installations.

⚠

**Caution**    If you upgrading from a TCC-I card to a TCC2 card, you must resolve this condition before you begin the upgrade. The TCC2 card does not compensate for reversed polarity.

### Procedure:  Clear the LAN-POL-REV Condition

**Step 1**    Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 2**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.114  LASEREOL

- Minor (MN), Non-Service Affecting (NSA)

The Laser Approaching End of Life alarm applies to TXP and MXP cards. It is typically accompanied by HI-LASERBIAS, page 2-83. It is an indicator that the laser in the card will need to be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100%, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100% and is accompanied by data errors, the card must be replaced sooner.

### Procedure:  Clear the LASEREOL Alarm

**Step 1**    Complete the "Physically Replace a Card" procedure on page 2-169.

⚠

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

**Step 2**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.115  LKOUTPR-S

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lockout of Protection Span 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 2-165.

**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).

## 2.6.116  LMP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)

The Link Management Protocol (LMP) Hello Down alarm occurs when the Hello protocol, which monitors UCP control channel status, is not available for link management. The unavailability can be caused by physical layer errors (such as cabling) or by control channel misconfiguration.

## Procedure:  Clear the LMP-HELLODOWN Alarm

**Step 1**  Verify that transmit and receive cables are not crossed at each end (login site and neighbor site).

**Step 2**  Verify there is no LOF (OC-N) alarm on the source or destination nodes. If there is complete the "Clear the LOS (DS-3) Alarm" procedure on page 2-103.

**Step 3**  If the alarm does not clear, complete the "Clear the CKTDOWN Alarm" procedure on page 2-43 to verify that IPCC provisioning is valid on both ends of the UNI.

**Step 4**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.117  LMP-NDFAIL

- Minor (MN) Non-Service Affecting (NSA)

The LMP Neighbor Detection Fail alarm occurs when neighbor detection within the UCP has failed. LMP-NDFAIL can be caused by physical failure (such as cabling) between the neighbors or by control channel misconfiguration.

## Procedure:  Clear the LMP-NDFAIL Alarm

**Step 1**  Complete the "Clear the LMP-HELLODOWN Alarm" procedure on page 2-92.

**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).

## 2.6.118 LOCKOUT-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lockout Switch Request on Facility/Equipment condition occurs when a user initiates a lock out switch request for an OC-N card or a lock out switch request on a path protection configuration 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 Path Protection Lock Out" procedure on page 2-166.

**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 LOCKOUT-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Lockout Switch Request 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 2-165.

**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 LOF (BITS)

- Major (MJ), Service Affecting (SA)

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC+/TCC2 BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data.

⚠️

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

✎

**Note**    The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turnup.

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

## Procedure:  Clear the LOF (BITS) Alarm

**Step 1**    Verify that the line framing and line coding match between the BITS input and the TCC+/TCC2:

**a.**    In node view or card view, note the slot and port reporting the alarm.

**b.**    Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.

**c.**    Click the **Provisioning > Timing** tabs to display the General Timing window.

**d.**    Verify that Coding matches the coding of the BITS timing source, either B8ZS or AMI.

**e.**    If the coding does not match, click **Coding** and choose the appropriate coding from the pull-down menu.

**f.**    Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

**g.**    If the framing does not match, click **Framing** and choose the appropriate framing from the pull-down menu.

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

**Step 2**    If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC+/TCC2, complete the "Physically Replace a Card" procedure on page 2-169 for the TCC+/TCC2 card.

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

**Step 3**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.121  LOF (DS-1)

- Major (MJ), Service Affecting (SA)

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream. If the LOF appears on the DS1-N-14 card, the transmitting equipment might have its framing set to a format that differs from the receiving ONS 15454.

## Procedure:  Clear the LOF (DS-1) Alarm

**Step 1**    Verify that the line framing and line coding match between the DS1-N-14 port and the signal source:

**a.**    In CTC, note the slot and port reporting the alarm.

**b.**    Find the coding and framing formats of the signal source for the card reporting the alarm. You might need to contact your network administrator for the format information.

**c.**    Display the card view of the reporting card.

    **d.**  Click the **Provisioning > Line** tabs.

    **e.**  Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the Line Type cell to reveal a pull-down menu and choose the matching type.

    **f.**  Verify that the reporting Line Coding matches the signal source's line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the Line Coding cell and choose the right type from the pull-down menu.

    **g.**  Click **Apply**.

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

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

**Step 2**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.122  LOF (DS-3)

- Critical (CR), Service Affecting (SA)

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment might be set to a format that differs from the receiving ONS 15454. On DS3XM-6 cards, the alarm occurs only on cards with the provisionable framing format set to C-bit or M13 and not on cards with the provisionable framing format is set to unframed.

## Procedure:  Clear the LOF (DS-3) Alarm

**Step 1**    Change the line type of the non-ONS equipment attached to the reporting card to C-bit:

    **a.**  Display the card view of the reporting card.

    **b.**  Click the **Provisioning > Line** tabs.

    **c.**  Verify that the line type of the reporting port matches the line type of the signal source.

    **d.**  If the signal source line type does not match the reporting port, click **Line Type** and choose **C-bit** from the pull-down menu.

    **e.**  Click **Apply**.

**Step 2**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.123  LOF (EC-N)

- Critical (CR), Service Affecting (SA)

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

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

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

### Procedure:  Clear the LOF (EC-N) Alarm

**Step 1**    Verify cabling continuity to the port reporting the alarm.

**Step 2**    If cabling continuity is OK, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 3**    If the alarm does not clear, see the "Network Troubleshooting Tests" section on page 1-2 to isolate the fault causing the LOF alarm.

**Step 4**    If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.124  LOF (OC-N)

- Critical (CR), Service Affecting (SA)

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

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

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

### Procedure:  Clear the LOF (OC-N) Alarm

**Step 1**    Verify cabling continuity to the port reporting the alarm.

**Step 2**    If cabling continuity is OK, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 3** If the alarm does not clear, see the "Network Troubleshooting Tests" section on page 1-2 to isolate the fault causing the LOF alarm.

**Step 4** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.125 LO-LASERBIAS

- Minor (MN), Non-Service Affecting (NSA)

The Equipment Low Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the minimum laser bias tolerance.

If the LO-LASERBIAS alarm threshold is set at 0% (the default), the laser's usability has ended. If the threshold is set at 5% to10%, the card is still usable for several weeks or months before you need to replace it.

### Procedure:  Clear the LO-LASERBIAS Alarm

**Step 1** Complete the "Clear the LASEREOL Alarm" procedure on page 2-91.

Replacement is not urgent and can be scheduled during a maintenance window.

**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).

## 2.6.126 LO-LASERTEMP

- Minor (MN), Non-Service Affecting (NSA)

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls 2° C under the card default level.

**Note** To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

### Procedure: Clear the LO-LASERTEMP Alarm

**Step 1** Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting MXP or TXP card.

**Step 2** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

⚠

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

**Step 3**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.127  LOM

- Critical (CR), Service Affecting (SA)

The Loss of Multiframe alarm applies to MXP and TXP cards when the MFAS overhead field is errored for more than five frames and persists for more than three milliseconds.

## Procedure:  Clear the LOM Alarm

**Step 1**    Complete the "Clear the SD Condition" procedure on page 2-140.

**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).

# 2.6.128  LOP-P

- Critical (CR), Service Affecting (SA)

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

⚠

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

## Procedure:  Clear the LOP-P Alarm

**Step 1**    In the node view, click the **Circuits** tab and view the alarmed circuit.

**Step 2**    Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS 3c instead of an STS1, this will cause the alarm.

**Step 3**   If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.

**Step 4**   If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-167.

**Step 5**   Recreate the circuit for the correct size. For instructions, see the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 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).

# 2.6.129  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.

⚠️

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

## Procedure:  Clear the LOP-V Alarm

**Step 1**   Complete the "Clear the LOP-P Alarm" procedure on page 2-98.

**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).

# 2.6.130  LO-RXPOWER

- Minor (MN), Non-Service Affecting (NSA)

The Equipment Low Receive Power alarm is an indicator for TXP card and MXP card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls under the threshold. The threshold value is user-provisionable.

## Procedure:  Clear the LO-RXPOWER Alarm

**Step 1**   At the transmit end of the errored circuit, increase the transmit power level within safe limits.

**Step 2**   Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.

✎

**Note**    If the card is part of an amplified dense wavelength multiplexing system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

**Step 3**    Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification will also cause channel power to need adjustment.

**Step 4**    If the alarm does not clear, remove any receive fiber attenuators, or replace them with lower-resistance attenuators.

**Step 5**    If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 6**    If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility loopback on a known-good port. The error readings you get will not be as precise, but you will generally know whether the fiber is faulty.

For specific procedures to use the test set equipment, consult the manufacturer.

**Step 7**    If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5.

**Step 8**    If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Card" procedure on page 2-169. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

⚠

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

**Step 9**    If no ports are shown bad and the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.131  LO-RXTEMP

- Minor (MN), Non-Service Affecting (NSA)

The Equipment Low Receive temperature alarm refers to the temperature of the trunk card port for the TXP and MXP cards. The LO-RXTEMP threshold is user-provisionable. The alarm does not occur unless the RxTemp Low threshold is set above 0° F or C.

## Procedure: Clear the LO-RXTEMP Alarm

**Step 1**    If this alarm accompanies other receive or transmit alarms for power, troubleshoot these alarms first.

**Step 2**    If the alarm does not clear, display the MXP or TXP card view.

**Step 3**    Click the **Provisioning > Optical Thresholds** tabs.

**Step 4**    Adjust the temperature in the Rx Temp Low column down a few degrees.

**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).

## 2.6.132 LOS (BITS)

- Major (MJ), Service Affecting

The LOS (BITS) alarm indicates that the TCC+/TCC2 card has an LOS from the BITS timing source. The LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.

⚠️

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

### Procedure:  Clear the LOS (BITS) Alarm

**Step 1**    Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.

**Step 2**    If wiring is OK, 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).

## 2.6.133 LOS (DS-1)

- Major (MJ), Service Affecting (SA)

A LOS (DS-1) alarm for a DS-3 port or a DS-1 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

⚠️

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

### Procedure:  Clear the LOS (DS-1) Alarm

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

**Step 2**    If the cabling is OK, verify that the correct port is in service:

    **a.**    Confirm that the OC-N card shows a green LED in CTC or on the physical card.

        A green LED indicates an active card. An amber LED indicates a standby card.

    **b.**    To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

     **c.** Click the **Provisioning > Line** tabs.

     **d.** Verify that the **State** column lists the port as IS.

     **e.** If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 3** If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 4** If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

**Step 5** If a valid signal exists, replace the DS-N connector on the ONS 15454.

**Step 6** Repeat Steps 1–5 for any other port on the card that reports the LOS (DS-1).

**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 (DS-1), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

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

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

**Step 9** If the alarm does not clear, log 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  LOS (DS-3)

• Critical (CR), Service Affecting (SA)

The LOS (DS-3) for either a DS-3 port or a DS-1 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

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

**Note** If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place 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 OK, verify that the correct port is in service:

   **a.**   Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green LED indicates an active card. An amber LED indicates a standby card.

   **b.**   To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

   **c.**   Click the **Provisioning > Line** tabs.

   **d.**   Verify that the **State** column lists the port as IS.

   **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 3**    If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line.

   For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 4**    If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

**Step 5**    If a valid signal exists, replace the DS-N connector on the ONS 15454.

**Step 6**    Repeat Steps 1–5 for any other port on the card that reports the LOS (DS-3).

**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 (DS-3), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

⚠

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

✎

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

**Step 9**    If the alarm does not clear, log 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  LOS (EC-N)

   • Critical (CR), Service Affecting (SA)

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

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

> ✎ **Note**    If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place 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 (EC-N) Alarm

**Step 1**    Verify cabling continuity to the port reporting the alarm.

**Step 2**    If the cabling is OK, verify that the correct port is in service:

   **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 correct port is in service, use an optical test set to confirm that a valid signal exists on the line.

   For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 4**    If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

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

**Step 6**    Repeat Steps 1–5 for any other port on the card that reports the LOS (EC-N).

**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 (EC-N), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

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

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

**Step 9**    If the alarm does not clear, log 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  LOS (OC-N)

- Critical (CR), Service Affecting (SA)

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

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

⚠ **Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

✎ **Note**    If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place 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 OK, verify that the correct port is in service:

    **a.**    Confirm that the OC-N card shows a green LED in CTC or on the physical card.

       A green LED indicates an active card. An amber LED indicates a standby card.

    **b.**    To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

    **c.**    Click the **Provisioning > Line** tabs.

    **d.**    Verify that the **State** column lists the port as IS.

    **e.**    If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 3**    If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 4**    If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "Optical Card Transmit and Receive Levels" section on page 1-84 lists these specifications for each card.

**Step 5**    If optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 6**    If a valid signal exists, replace the connector on the backplane.

**Step 7**    Repeat Steps 1–6 for any other port on the card reporting the LOS (OC-N).

**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 (OC-N), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

⚠️

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

✎

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

**Step 10**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.137  LO-TXPOWER

- Minor (MN), Non-Service Affecting (NSA)

The Equipment Low Transmit Power alarm is an indicator for TXP card and MXP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

### Procedure:  Clear the LO-TXPOWER Alarm

**Step 1**    Display the MXP or TXP card view.

**Step 2**    Click the **Provisioning > Optical Thresholds** tabs.

**Step 3**    Increase the TX Power Low column value by 0.5 dBm.

**Step 4**    If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Card" procedure on page 2-169.

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

**Step 5**    If 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  LPBKCRS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between a traffic (optical) card and a cross-connect card. A cross-connect loopback is a sub-line speed test that does not affect traffic.

For more information on loopbacks, see the .

## Clear the LBKCRS Condition

**Step 1**    To remove the loopback cross-connect condition, double-click the traffic (optical) card in CTC to display the card view.

**Step 2**    Click the **Provisioning > SONET STS** tabs.

**Step 3**    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.

# 2.6.139  LPBKDS1FEAC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

## Procedure: Clear the LPBKDS1FEAC Condition

**Step 1**    At the node view, double-click the DS3XM-6 card to display the card view.

**Step 2**    Click the **Maintenance > DS1** tabs.

**Step 3**    Click the Send Code column, cell for the port and click **No Code** from the pull-down menu.

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

**Step 4** 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.

## 2.6.140  LPBKDS1FEAC-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-1 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-1 FEAC loopback. For more information about FEAC loopbacks, see the "Using the DS3XM-6 Card FEAC (Loopback) Functions" section on page 1-22.

**Note** LPBKDS1FEAC-CMD is an informational condition. It does not require troubleshooting.

## 2.6.141  LPBKDS3FEAC

- Not Alarmed (NA), Non-Service Affecting (NSA)

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6 card loopback signal is received from the far-end node because of a Far-End Alarm and Control (FEAC) command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by DS3XM-6 cards. and DS3-12E cards. A DS3XM-6 card both generates and reports FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

**Caution** CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

**Note** LPBKDS3FEAC is an informational condition. It does not require troubleshooting.

### Procedure: Clear the LPBKDS3FEAC Condition

**Step 1** At the node view, double-click the DS3XM-6 card to display the card view.

**Step 2** Click the **Maintenance > DS3** tabs.

**Step 3** Click the Send Code column, cell for the port and click **No Code** from the pull-down menu.

**Step 4** 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.

## 2.6.142  LPBKDS3FEAC-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The DS-3 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-3 FEAC loopback. For more information about FEAC loopbacks, see the "Using the DS3XM-6 Card FEAC (Loopback) Functions" section on page 1-22.

**Note**    LPBKDS3FEAC-CMD is an informational condition. It does not require troubleshooting.

## 2.6.143 LPBKFACILITY (DS-1 or DS-3)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A 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 "Network Troubleshooting Tests" section on page 1-2 or the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-5.

**Caution**    CTC permits you to perform loopbacks on an in-service (IS) circuit, but performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or force switch to protect traffic, the LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS.

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

### Procedure:  Clear the LPBKFACILITY (DS-1 or DS-3) Condition

**Step 1**    From the node view, double-click the reporting DS3XM-6 card to display the card view.

**Step 2**    Click the **Maintenance > DS3** tab.

If the condition is reported against a DS-1 line, also click the **DS1** tab.

**Step 3**    Complete the "Clear a Loopback" procedure on page 2-167.

**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 LPBKFACILITY (EC-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A 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 "Network Troubleshooting Tests" section on page 1-2 or the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-5.

⚠️ **Caution**   CTC permits you to perform loopbacks on an in-service (IS) circuit, but performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or force switch to protect traffic, the LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS..

## Procedure:  Clear the LPBKFACILITY (EC-N) Condition

**Step 1**   The loopback originates from the DS3XM-6 card. Complete the "Clear the LPBKDS3FEAC Condition" procedure on page 2-108.

**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).

# 2.6.145  LPBKFACILITY (OC-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A 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 1-23.

⚠️ **Caution**   CTC permits you to perform loopbacks on an in-service (IS) circuit, but performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or force switch to protect traffic, the LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS.

## Procedure:  Clear the LPBKFACILITY (OC-N) Condition

**Step 1**   Complete the "Clear a Loopback" procedure on page 2-167.

**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 non-looped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N.

# 2.6.146  LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N)

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

**Note**    Performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For more information about loopbacks, see the "Network Troubleshooting Tests" section on page 1-2.

## Procedure:  Clear the LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N) Condition

**Step 1**    Complete the "Clear a Loopback" procedure on page 2-167.

**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).

**Note**    Terminal loopback is not supported at the DS-1 level for the DS3XM-6 card.

# 2.6.147  LPBKTERMINAL (G-Series)

- Not Alarmed (NA), Non-Service Affecting (NSA)

A 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 G1000-4 card the outgoing signal is not transmitted; it is only redirected in the receive direction. G1000-4 cards only support terminal loopbacks.

**Note**    Performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For more information about loopbacks, see the "Network Troubleshooting Tests" section on page 1-2.

## Procedure:  Clear the LPBKTERMINAL (G-Series) Condition

**Step 1**    Complete the "Clear a Loopback" procedure on page 2-167.

**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).

## 2.6.148  MAN-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

### Procedure:  Clear the MAN-REQ Condition

**Step 1**    Complete the "Clear a Path Protection Lock Out" procedure on page 2-166.

**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).

## 2.6.149  MANRESET

- Not Alarmed (NA), Non-Service Affecting (NSA)

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

**Note**    MANRESET is an informational condition. It does not require troubleshooting.

## 2.6.150  MANSWTOINT

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to the internal timing source.

**Note**    MANSWTOINT is an informational condition. It does not require troubleshooting.

## 2.6.151  MANSWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

**Note**    MANSWTOPRI is an informational condition. It does not require troubleshooting.

## 2.6.152 MANSWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to the second timing source.

**Note** MANSWTOSEC is an informational condition. It does not require troubleshooting.

## 2.6.153 MANSWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the tertiary timing source.

**Note** MANSWTOTHIRD is an informational condition. It does not require troubleshooting.

## 2.6.154 MANUAL-REQ-RING

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on two-fiber and four-fiber BLSR rings to switch from working to protect or protect to working.

### Procedure: Clear the MANUAL-REQ-RING Condition

**Step 1** Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

**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).

## 2.6.155 MANUAL-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Manual Switch Request on Ring condition occurs on four-fiber BLSRs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span.

### Procedure: Clear the MANUAL-REQ-SPAN Condition

**Step 1** Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

**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).

## 2.6.156  MEA (AIP)

- Critical (CR), Service Affecting (SA)

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the Alarm Interface Panel (AIP), the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-Amp fuse is installed in a newer 10 Gbps-compatible or ANSI shelf assembly (15454-SA-ANSI).

### Procedure:  Clear the MEA (AIP) Alarm

**Step 1**   Complete the "Replace the Alarm Interface Panel" procedure on page 3-12.

**Step 2**   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.157  MEA (BP)

- Critical (CR), Service Affecting (SA)

The MEA alarm for the backplane occurs when the revision of the backplane is incompatible with cross-connect equipment.

### Procedure:  Clear the MEA (BP) Alarm

**Step 1**   If the MEA is also raised against other equipment, such as the AIP or a fan-tray assembly, troubleshoot these alarms first.

**Step 2**   If alarms are reported directly against the cross-connect card, such as SWMTXMOD, page 2-150, troubleshoot these alarms next.

**Step 3**   If the alarm does not clear, determine whether the ONS 15454 shelf assembly is a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) or an earlier shelf assembly:

   **a.**   At the node view, click the **Inventory** tab.

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

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

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

**Step 4**    If the shelf assembly is not compatible with 10-Gbps equipment, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.158  MEA (EQPT)

- Critical (CR), Service Affecting (SA)

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

**Note**    If an OC3-8 card is installed in a high-speed slot (Slots 5-6 and 12-13), it will not appear in CTC and will raise an MEA.

## Procedure:  Clear the MEA (EQPT) Alarm

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

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

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

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

**Step 2**    Physically verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card's faceplate.

   **a.**    If you have a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 3.

   **b.**    If you have a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet (traffic) card is incompatible and must be removed.

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

     **c.**  If you have a pre-ANSI shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the XC10G, OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to Step 3.

     **d.**  If you have a pre-ANSI shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the XC10G, OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed.

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

**Step 4**    If you prefer the card type depicted by CTC, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

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

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

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

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

**Step 6**    If any ports on the card are in service, take them out of service (OOS):

⚠ **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 7**    If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-167.

⚠ **Caution**    Before deleting the circuit, ensure that live traffic is not present.

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

     **a.**  Click the **Provisioning > Protection** tabs.

     **b.**  Choose the protection group of the reporting card.

     **c.**  Click **Delete**.

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

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

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

**Step 11**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.159  MEA (FAN)

- Critical (CR), Service Affecting (SA)

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

### Procedure:  Clear the MEA (FAN) Alarm

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

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

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

**Step 2**    If you have a 15454-SA-ANSI shelf or 10-Gbps compatible shelf assembly, the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5 Amp fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

**Step 3**    If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

**Step 4**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.160  MEM-GONE

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

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC+/TCC2 card. CTC does 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).

## 2.6.161  MEM-LOW

- Minor (MN), Non-Service Affecting (NSA)

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC+/TCC2 card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC+/TCC2 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).

## 2.6.162  MFGMEM

- Critical (CR), Service Affecting (SA)

The MFGMEM or Manufacturing Data Memory Failure alarm occurs if the ONS 15454 cannot access the data in the erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC+/TCC2 lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EEPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address disrupts IP connectivity and grays out the ONS 15454 icon on the CTC network view.

### Procedure:  Clear the MFGMEM (AIP, BP, Fan-Tray Assembly) Alarm

**Step 1**  Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 2**  If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

**Step 3**  If the MFGMEM alarm continues to report after replacing the TCC+/TCC2 cards, the problem is with the EEPROM.

**Step 4**  If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

**Step 5**  If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

**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).

## 2.6.163  NO-CONFIG

- Not Alarmed (NA), Non-Service Affecting (NSA)

The No Startup Configuration alarm applies to ML-series Ethernet (traffic) cards and occurs when you pre-provision a high-speed slot (Slots 5-6 and 12-13) for the card without inserting the card first, or when you insert a card without pre-provisioning. (This is an exception to the usual rule in card provisioning.) Because this is normal operation, you should expect this alarm during provisioning. When the startup configuration file is copied to the active TCC+/TCC2, the alarm clears.

### Procedure:  Clear the NO-CONFIG Alarm

**Step 1**    Create a startup configuration for the card in IOS.

Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

**Step 2**    Upload the configuration file to the TCC+/TCC2:

   **a.**  In the node view, right-click the ML card graphic.

   **b.**  Choose **IOS Startup Config** from the shortcut menu.

   **c.**  Click **Upload to TCC** and navigate to the file location.

**Step 3**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169.

**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).

## 2.6.164  NOT-AUTHENTICATED

- Default Severity: Minor (MN), Non-Service-Affecting (NSA)

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred.

**Note**    NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

## 2.6.165  ODUK-AIS-PM

- Not Reported (NR), Non-Service Affecting (NSA)

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. It is a secondary condition that indicates a more serious condition such as LOS (OC-N), page 2-105, is occurring downstream. The ODUK-AIS-PM condition is reported in the path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by an ODUK-OCI-PM, page 2-121, upstream.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the ODUK-AIS-PM Condition

**Step 1**    Verify whether upstream nodes and equipment have alarms, especially an LOS (OC-N), page 2-105, or OOS ports.

**Step 2**    Clear the upstream alarms using the applicable procedure(s) 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).

# 2.6.166  ODUK-BDI-PM

- Not Reported (NR), Non-Service Affecting (NSA)

The ODUK Backward Defect Indicator (BDI) PM condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead. ODUK-BDI-PM occurs when a PORT-CODE-MISM, page 2-130, occurs upstream.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the ODUK-BDI-PM Condition

**Step 1**    Complete the "Clear the OTUK-BDI condition" procedure on page 2-123.

**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).

# 2.6.167  ODUK-LCK-PM

- Not Reported (NR), Non-Service Affecting (NSA)

The ODUK Locked Defect (LCK) PM condition applies to TXP and MXP cards when G.709 monitoring is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the ODUK-LCK-PM Condition

**Step 1**    Unlock the upstream node signal.

**Step 2**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.168  ODUK-OCI-PM

- Not Reported (NR), Non-Service Affecting (NSA)

The ODUK Open Connection Indication (OCI) PM condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes an ODUK-LCK-PM, page 2-120, downstream.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure:  Clear the ODUK-OCI-PM Condition

**Step 1**    Verify the fiber connectivity at nodes upstream.

**Step 2**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.169  ODUK-SD-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)

The ODUK Signal Degrade (SD) PM condition applies to TXP cards and MXP cards when G.709 monitoring is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure:  Clear the ODUK-SD-PM Condition

**Step 1**    Complete the "Clear the SD Condition" procedure on page 2-140.

**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).

# 2.6.170  ODUK-SF-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the ODUK-SF-PM Condition

**Step 1**   Complete the "Clear the SF Condition" procedure on page 2-142.

**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).

# 2.6.171  ODUK-TIM-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)

The ODUK Trace Identifier Mismatch (TIM) PM condition applies to the path monitoring area of the optical transport network (OTN) overhead for TXP cards and MXP cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an ODUK-BDI-PM, page 2-120, downstream.

The ODUK-TIM-PM condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the ODUK-TIM-PM Condition

**Step 1**   Complete the "Clear the TIM-P Alarm" procedure on page 2-156.

**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).

## 2.6.172  OTUK-AIS

- Not Reported (NR), Non-Service Affecting (NSA)

The Optical Transport Unit (OTUK) AIS condition applies to transponder (TXP) cards and muxponder (MXP) cards when G.709 monitoring is enabled for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition such as an LOS (OC-N), page 2-105, is occurring downstream. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure:  Clear the OTUK-AIS Condition

**Step 1**    Complete the "Clear the AIS Condition" procedure on page 2-21.

**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).

## 2.6.173  OTUK-BDI

- Not Reported (NR), Non-Service Affecting (NSA)

The OTUK BDI condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. OTUK-BDI is indicated by the BDI bit in the section monitoring overhead. The alarm occurs when there is an SF, page 2-141, upstream. OTUK-BDI is triggered by a OTUK-TIM, page 2-125.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure:  Clear the OTUK-BDI condition

**Step 1**    Verify whether upstream nodes have an OTUK-AIS, page 2-123.

**Step 2**    In the upstream node, click the MXP or TXP card in the node view to display the card view.

**Step 3**    Click the **Provisioning > OTN > Trail Trade Identifier** tabs.

**Step 4**    Compare the Current Transmit String with the Current Expected String in the downstream node. (Verify the Current Expected String by making the same navigations in another CTC session to the downstream node.)

**Step 5**    If the two do not match, modify the Current Expected String.

**Step 6**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.174  OTUK-IAE

- Major (MJ), Service Affecting (SA)

The OTUK Incoming Alignment Error (IAE) alarm applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. OTUK-IAE refers to a single bit that allows the input port to notify the output port that the incoming signal has an alignment error. The error is indicated in the section monitoring overhead of the digital wrapper.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Clear the OTUK-IAE Condition

**Step 1**  OTUK-IAE indicates an internal problem in the reporting card. Complete the "Physically Replace a Card" procedure on page 2-169.

⚠

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

**Step 2**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.175  OTUK-LOF

- Critical (CR), Service Affecting (SA)

The OTUK-LOF alarm applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure: Clear the OTUK-LOF Alarm

**Step 1**  Complete the "Clear the LOF (OC-N) Alarm" procedure on page 2-96.

**Step 2**  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).

## 2.6.176  OTUK-SD

- Not Alarmed (NA) Non-Service Affecting (NSA)

The OTUK-SD condition applies to TXP cards and MXP cards when G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure: Clear the OTUK-SD Condition

**Step 1**   Complete the "Clear the SD Condition" procedure on page 2-140.

**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  OTUK-SF

- Not Alarmed (NA), Non-Service Affecting (NSA)

The OTUK-SF condition applies to TXP cards and MXP cards when G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

### Procedure: Clear the OTUK-SF Condition

**Step 1**   Complete the "Clear the SD Condition" procedure on page 2-140.

**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).

## 2.6.178  OTUK-TIM

- Minor (MN), Non-Service Affecting (NSA)

The OTUK-TIM alarm applies to TXP cards and MXP cards when G.709 monitoring is enabled and section trace mode is set to manual. The alarm indicates that the expected TT1 string does not match the received TTI string in the optical transport unit overhead of the digital wrapper. OTUK-TIM triggers an ODUK-BDI-PM, page 2-120.

G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure: Clear the OTUK-TIM Alarm

**Step 1**    Complete the "Clear the TIM-P Alarm" procedure on page 2-156.

**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).

## 2.6.179  PDI-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

The ONS 15454 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS, page 2-21, often accompanies the PDI-P condition. If the PDI-P is the only condition reported with the AIS, clear the PDI-P condition to clear the AIS condition. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on the port of an OC-N card supporting a G1000-4 card circuit might result from the end-to-end Ethernet link integrity feature of the G1000-4. If the link integrity is the cause, it typically is accompanied by an TPTFAIL (G-Series), page 2-156, or a CARLOSS (G-Series), page 2-39, reported against one or both Ethernet ports terminating the circuit. If TPTFAIL or CARLOSS are reported against one or both of the Ethernet ports, troubleshooting the accompanying alarm clears the PDI-P condition.

A PDI-P condition reported on the port of an OC-N card supporting an ML-series card circuit might result from the end-to-end Ethernet link integrity feature of the ML-series card. If the link integrity is the cause, it typically is accompanied by a TPTFAIL (G-Series) reported against one or both packet over SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for more information about ML-series cards.

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

**Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the PDI-P Condition

**Step 1**    Verify that all circuits terminating in the reporting card are in an active state:

    **a.**    Click the **Circuits** tab.

    **b.**    Verify that the **State** column lists the port as active.

    **c.**    If the State column lists the port as incomplete, wait 10 minutes for the ONS 15454 to 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 2-167.

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

**Step 4**    Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

**Step 5**    If circuit deletion and recreation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

**Step 6**    If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

**Step 7**    If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 8**    If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the optical/electrical (traffic) cards.

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

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

**Step 9**    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.180  PEER-NORESPONSE

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

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

### Procedure:  Clear the PEER-NORESPONSE Alarm

**Step 1**  Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

**Step 3**  Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

**Step 5**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.181  PLM-P

- Critical (CR), Service Affecting (SA)

A Payload Label Mismatch Path 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 condition can occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card will transmit this value, but a DS-3 card will transmit a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

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

⚠ **Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the PLM-P Alarm

**Step 1**    Verify that all circuits terminating in the reporting card are active:

   **a.**  Click the **Circuits** tab.

   **b.**  Verify that the **State** column lists the port as active.

   **c.**  If the State column lists the port as incomplete, wait 10 minutes for the ONS 15454 to 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 2-167.

⚠ **Caution**    Deleting a circuit might affect traffic.

**Step 4**    Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

**Step 5**    If the circuit deletion and recreation does not clear the alarm, verify the far-end OC-N card that provides STS payload to the DS-N card.

**Step 6**    If the alarm does not clear, verify the cross-connect between the OC-N card and the DS-N card.

**Step 7**    If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 8**    If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting traffic card.

⚠️

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

✎

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

**Step 9**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.182  PLM-V

- Minor (MN), Service Affecting (SA)

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

## 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).

# 2.6.183  PORT-CODE-MISM

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

The Pluggable Port Security Code Mismatch alarm refers to ML-series Ethernet (traffic) cards, MXPs, and TXPs. PORT-CODE-MISM occurs when the SFP connector that is plugged into the card is not supported by Cisco.

## Procedure:  Clear the PORT-CODE-MISM Alarm

**Step 1**    Unplug the SFP connector and fiber from the reporting card.

**Step 2**    If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

**Step 3**    Pull the fiber cable straight out of the connector.

Step 4    Plug the fiber into a Cisco-supported SFP connector.

Step 5    If the new SFP connector has a latch, close the latch over the cable to secure it.

Step 6    Plug the cabled SFP connector into the card port until it clicks.

Step 7    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.184  PORT-COMM-FAIL

- Major (MJ), Service Affecting (SA)

The Port Communication Failure alarm applies to TXP and MXP card SFPs. It occurs when the card cannot communicate with the SFP.

## Procedure:  Clear the PORT-COMM-FAIL Alarm

Step 1    Replace the faulty SFP with a new SFP:

　　a.　Unplug the SFP connector and fiber from the ML-series Ethernet (traffic) card.

　　b.　If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

　　c.　Pull the fiber cable straight out of the connector.

　　d.　Plug the fiber into a Cisco-supported SFP connector.

　　e.　If the new SFP connector has a latch, close the latch over the cable to secure it.

　　f.　Plug the cabled SFP connector into the ML-series Ethernet card port until it clicks.

Step 2    If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (TAC) at 1-800-553-2447.

# 2.6.185  PORT-MISMATCH

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

The Pluggable Port Mismatch alarm applies to ML-series Ethernet (traffic) card SFP connectors. The alarm indicates that the provisioned payload for the connector does not match the SFP configuration.

The error must be resolved in the IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*. 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  PORT-MISSING

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

The Pluggable Port Code Missing alarm applies to ML-series Ethernet (traffic) card SFP connectors. The alarm indicates that the connector is not plugged into the card port.

For information about provisioning the ML-series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

## Procedure:  Clear the PORT-MISSING Alarm

**Step 1**    If fiber is not plugged into the SFP connector, plug it in.

**Step 2**    If the SFP connector has a latch, pull the latch over the connector.

**Step 3**    Push the SFP connector into the ML-series Ethernet (traffic) card port until it clicks in place.

**Step 4**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

# 2.6.187  PRC-DUPID

- Major (MJ), Service Affecting (SA) for Ring
- Major (MJ), Non-Service Affecting (NSA) for NE

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

## Procedure:  Clear the PRC-DUPID Alarm

**Step 1**    Log into a node on the ring.

**Step 2**    Find the node ID by completing the "Identify a Ring ID or Node ID Number" procedure on page 2-164.

**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 2-164 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).

# 2.6.188  PROTNA

- Minor (MN), Non-Service Affecting (NSA)

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC+/TCC2 or cross-connect card that is provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

## Procedure:  Clear the PROTNA Alarm

**Step 1**    If the PROTNA alarm occurs and does not clear, and if it is raised against a common control card (TCC+/TCC2 or cross-connect), ensure that there is a redundant control card installed and provisioned in the chassis.

**Step 2**    If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS):

    **a.**    In CTC, double-click the reporting card to display the card view (if the card is not a cross-connect card).

    **b.**    Click the **Provisioning** tab.

    **c.**    Click the **State** of any in-service (IS) ports.

    **d.**    Choose **OOS** to take the ports out of service.

**Step 3**    Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 15454, the ACT/STBY LED is illuminated.

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

**Step 5**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

**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).

# 2.6.189  PWR-A

- Minor (MN), Non-Service Affecting (NSA)

The NE Power (PWR) Failure At Connector A alarm applies to the NE shelf. It occurs when there is no power supplied to the main power connector. PWR-A can occur if power is connected to the backup power connector (Connector B) but not to Connector A, because power must be applied to both supplies.

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

## Procedure:  Clear the PWR-A Alarm

**Step 1**    Ensure that a power connection is present between the power source and power connector A.

**Step 2**    If necessary, reseat the connections between the source and the power connector A.

**Step 3**   If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

**Step 4**   If the alarm does not clear, verify the source power output with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

**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).

# 2.6.190  PWR-B

- Minor (MN), Non-Service Affecting (NSA)

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

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

## Procedure:  Clear the PWR-B Alarm

**Step 1**   Ensure that a power connection is present between the power source and power connector B.

**Step 2**   If necessary, reseat the connections between the source and power connector B.

**Step 3**   If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

**Step 4**   If the alarm does not clear, verify the source power output with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

**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).

# 2.6.191  PWR-REDUN

- Minor (MN), Non-Service Affecting (NSA)

The Redundant Power Capability Lost alarm applies to cards that have two built-in fuses (such as the TCC2 and newer optical (traffic) cards). The alarm indicates that one of the fuses has blown and must be serviced. When this alarm occurs, the card's power redundancy is lost because only one card power connection can contact one of the redundant power supplies.

## Procedure: Clear the PWR-REDUN Alarm

**Step 1**    The card fuse is not field-replaceable. Complete the "Physically Replace a Card" procedure on page 2-169.

⚠️

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

**Step 2**    Log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447) to arrange a card return for service.

## 2.6.192  RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on the DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS, page 2-21.

## Procedure:  Clear the RAI Condition

**Step 1**    Complete the "Clear the AIS Condition" procedure on page 2-21.

**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).

## 2.6.193  RCVR-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from the DS-1 port or a possible mismatch of backplane equipment occurs, for example, an SMB connector or a BNC connector is connected to a DS-1 card.

✎

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

⚠️

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

**Cisco ONS 15454 Troubleshooting Guide, R4.0**

## Procedure:  Clear the RCVR-MISS Alarm

**Step 1**    Ensure that the device attached to the DS-1 port is operational.

**Step 2**    If the attachment is OK, verify that the cabling is securely connected.

**Step 3**    If the cabling is OK, verify that the pinouts are correct.

**Step 4**    If the pinouts are correct, replace the receive cable.

**Step 5**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.194  RFI-L

- Not Reported (NR), Non-Service Affecting (NSA)

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

**Step 2**    Identify and clear any alarms, particularly LOS (OC-N), page 2-105.

**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).

# 2.6.195  RFI-P

- Not Reported (NR), Non-Service Affecting (NSA)

An RFI Path condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P 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 15454:

**a.**    Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

**b.**    To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

**c.**    Click the **Provisioning > Line** tabs.

    **d.**   Verify that the **State** column lists the port as IS.

    **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 2**    To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

**Step 3**    Clear alarms in the node with the failure, especially an UNEQ-P, page 2-159, or UNEQ-V, page 2-161.

**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).

# 2.6.196  RFI-V

- Not Reported (NR), Non-Service Affecting (NSA)

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

⚠️

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

## 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 15454 Procedure Guide*.

**Step 2**    If connectors are correctly connected, verify that the DS-1 port is active and in service (IS):

    **a.**   Confirm that the OC-N card shows a green LED in CTC or on the physical card.

       A green LED indicates an active card. An amber LED indicates a standby card.

    **b.**   To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

    **c.**   Click the **Provisioning > Line** tabs.

    **d.**   Verify that the **State** column lists the port as IS.

    **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 3**    If the ports are active and in service, use an optical test set to verify that the signal source does not have errors.

    For specific procedures to use the test set equipment, consult the manufacturer.

**Step 4**    If the signal is valid, log into the node at the far-end of the reporting ONS 15454.

**Step 5**    Clear alarms in the far-end node, especially an UNEQ-P, page 2-159, or UNEQ-V, page 2-161.

**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).

## 2.6.197 RING-MISMATCH

- Major (MJ), Service Affecting (SA)

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

### Procedure:  Clear the RING-MISMATCH Alarm

**Step 1**    In the 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 2-164.

**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 2-164.

**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).

## 2.6.198 RING-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

**Note**    RING-SW-EAST is an informational condition. It does not require troubleshooting.

## 2.6.199 RING-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

**Note**    RING-SW-WEST is an informational condition. It does not require troubleshooting.

## 2.6.200 RSVP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)

The Resource Reservation Protocol (RSVP) Hello Down alarm occurs when the Hello protocol, which monitors UCP control channel status, is not available for reserving resources. The lack of availability can be caused by misconfiguration or loss of connectivity between the reporting node and its neighbor.

### Procedure:  Clear the RSVP-HELLODOWN Alarm

**Step 1**    Ensure that there are no physical layer problems between the reporting node and its neighbor.

**Step 2**    Ensure that neighbor discovery (if enabled) has completed without any errors:

    **a.**    In the node CTC view, click the **Provisioning > UCP > Neighbor** tabs.

    **b.**    Look for the neighbor ID and address. If it is present, neighbor discovery is working.

**Step 3**    Ensure that RSVP hello is enabled on the neighbor node:

    **a.**    In the node view, click **View > Go to Network View**.

    **b.**    Double-click the neighbor node in the network map.

    **c.**    Click the **Provisioning > UCP > Node** tabs on this neighbor.

    **d.**    Ensure that the RSVP area of the window contains entries in the Restart Time, Retransmit Interval, Recovery Time, and Refresh Interval fields.

**Step 4**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.201  RUNCFG-SAVENEED

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML1000 and ML100T cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering **copy run start** at the CLI. If you do not save the change, the change is lost after the card reboots.

## 2.6.202  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 15454 is user provisionable and has a range for SD from $10^{-9}$ to $10^{-5}$.

SD-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SD 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**    **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

**Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the SD Condition

**Step 1**    Complete the "Verify BER Threshold Level" procedure on page 2-169.

**Step 2**    If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.

For specific procedures to use the test set equipment, consult the manufacturer.

**Step 3**    If the optical power level is OK, verify that optical receive levels are within the acceptable range.

**Step 4**    If receive levels are OK, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**Step 5**    If the condition does not clear, verify that single-mode fiber is used.

**Step 6**    If the fiber is the correct type, verify that a single-mode laser is used at the far-end node.

**Step 7**    If the problem does not clear, the transmitter at the other end of the optical line 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).

## 2.6.203  SD-L

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SD Line condition is similar to an SD, page 2-139. 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 2-140.

**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).

# 2.6.204  SD-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SD Path condition is similar to an SD, page 2-139, but it applies to the path (STS) layer of the SONET overhead. A path or ST- level SD alarm travels on the B3 byte of the SONET overhead.

For path protection configuration protected circuits, the BER threshold on the ONS 15454 is user provisionable and has a range for SD from $10^{-9}$ to $10^{-5}$. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to $10^{-6}$.

On path protection configuration, 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 2-140.

**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).

# 2.6.205  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, page 2-139, 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 15454 is user provisionable and has a range for SF from 10-5 to 10-3.

SF-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SF 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.

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

**Warning** **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the SF Condition

**Step 1** Complete the "Clear the SD Condition" procedure on page 2-140.

**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).

# 2.6.206  SF-L

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SF Line condition is similar to an SF, page 2-141, 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 2-140.

**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).

# 2.6.207  SF-P

- Not Alarmed (NA), Non-Service Affecting (NSA)

An SF Path condition is similar to an SF, page 2-141, but it applies to the path (STS) layer of the SONET overhead. A path or ST- level SD alarm travels on the B3 byte of the SONET overhead.

For path protection configuration circuits, the BER threshold on the ONS 15454 is user provisionable and has a range for SF from $10^{-5}$ to $10^{-3}$. For BLSR 1+1 or unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to $10^{-3}$.

For path protection configuration, 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 2-140.

**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).

# 2.6.208  SFTWDOWN

- Minor (MN), Non-Service Affecting (NSA)

A Software Download in Progress alarm occurs when the TCC+/TCC2 is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log onto http://www.cisco.com/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 TCC+/TCC2 card.

**Note**    SFTWDOWN is an informational alarm.

## 2.6.209 SNTP-HOST

- Minor (MN), Non-Service Affecting (NSA)

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

### Procedure:  Clear the SNTP-HOST Alarm

**Step 1**    Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

**Step 2**    If the ping fails, contact the network administrator who manages the IP network 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 15454.

**Step 3**    If no network problems exist, ensure that the ONS 15454 proxy is provisioned correctly:

    **a.**    In node view for the ONS node serving as the proxy, click the **Provisioning > General** tabs.

    **b.**    Ensure that the Use NTP/SNTP Server check box is checked.

    **c.**    If the Use NTP/SNTP Server check box is not checked, click it.

    **d.**    Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

**Step 4**    If proxy is correctly provisioned, refer to the *Cisco ONS 15454 Reference Manual* for more information on SNTP Host.

**Step 5**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.210 SPAN-SW-EAST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber BLSR span. The condition clears when the switch is cleared.

**Note**    SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

## 2.6.211 SPAN-SW-WEST

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span. The condition clears when the switch is cleared.

**Note**      SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

## 2.6.212  SQUELCH

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. AIS-P, page 2-22, also appears on all nodes in the ring except the isolated node.

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

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

**Warning**      **Invisible laser radiation 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 SQUELCH Condition

**Step 1**      Determine the isolated node:

   **a.**   In the 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 OK, verify that the proper ports are in service:

   **a.**   Confirm that the OC-N card shows a green LED in CTC or on the physical card.

         A green LED indicates an active card. An amber LED indicates a standby card.

   **b.**   To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

   **c.**   Click the **Provisioning > Line** tabs.

   **d.**   Verify that the **State** column lists the port as IS.

   **e.**   If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

**Step 4**      If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 5**   If the signal is valid, verify that the power level of the optical signal is within the optical (traffic) card's receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.

**Step 6**   If the receiver levels are OK, ensure that the optical transmit and receive fibers are connected properly.

**Step 7**   If the connectors are OK, complete the "Physically Replace a Card" procedure on page 2-169 for the OC-N card.

⚠

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

**Step 8**   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.213  SQUELCHED

- Major (MJ), Service Affecting (SA)

The DWDM Client Signal Squelched alarm is raised by an MXP or TXP card when G.709 monitoring is enabled and the card is operating in transparent mode. The alarm occurs on a far-end MXP or TXP client port when the near end detects an LOF (OC-N), page 2-96, or LOS (OC-N), page 2-105. The signal loss is indicated by an OTUK-AIS, page 2-123, in the OTN overhead. SQUELCHED can also indicate that the far-end trunk signal is invalid.

### Procedure:  Clear the SQUELCHED Alarm

**Step 1**   Verify that the far-end node and near-end node are not reporting an LOF (OC-N), page 2-96, or an LOS (OC-N), page 2-105. If so, complete the "Clear the LOF (OC-N) Alarm" procedure on page 2-96.

**Step 2**   If no LOF or LOS is reported, verify that the far-end node and near-end are not reporting a WVL-MISMATCH, page 2-162, for the trunk or DSP-FAIL, page 2-55. If either alarm is reported, complete the "Clear the WVL-MISMATCH alarm" procedure on page 2-162 or the "Clear the DSP-FAIL Alarm" procedure on page 2-55 as appropriate.

**Step 3**   If no WVL-MISMATCH or DSP-FAIL is reported, verify that the near-end port reporting the SQUELCHED alarm is in service and is not in loopback:

  **a.**   Double-click the client card to display the card view.

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

  **c.**   If the port State column says OOS or OOS_MT, click the cell to highlight it and choose **IS** from the pull-down menu. Changing the state to IS will also clear any loopback provisioned on the port.

**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).

## 2.6.214 SSM-DUS

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Status (SSM) Message 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.

## 2.6.215 SSM-FAIL

- Minor (MN), Non-Service Affecting (NSA)

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

### 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).

## 2.6.216 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.

**Note**    SSM-LNC is an informational condition. It does not require troubleshooting.

## 2.6.217 SSM-OFF

- Not Alarmed (NA), Non-Service Affecting (NSA)

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS 15454 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 2-147.

**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).

# 2.6.218 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.

**Note** SSM-PRC is an informational condition. It does not require troubleshooting.

# 2.6.219 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.

# 2.6.220 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.

# 2.6.221 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.

## 2.6.222  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.

## 2.6.223  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.

## 2.6.224  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.

## 2.6.225  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.

# 2.6.226  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 15454 has SSM support enabled. STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

## Procedure:  Clear the STU Condition

**Step 1**    In the 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).

# 2.6.227  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.

# 2.6.228  SWMTXMOD

- Critical (CR), Service Affecting (SA)

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

If the alarm reports against a cross-connect card, it occurs when a logic component internal to the reporting cross-connect card is out of frame with a second logic component on the same cross-connect card. One or more traffic cards might lose traffic as a result of the cross-connect frame failure.

## Procedure:  Clear the SWMTXMOD Alarm

**Step 1**    If the card reporting the alarm is the standby cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the 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 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 15454, the ACT/STBY LED is illuminated.

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

**Step 3**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the standby cross-connect card.

**Step 4**    If the card reporting the alarm is the active cross-connect card, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-166.

> ✎
> **Note**    After the active cross-connect goes into standby, the original standby slot becomes active. The former standby card ACT/STBY LED becomes green.

**Step 5**    If the card reporting the alarm is not the active cross-connect card or if you completed the side switch in Step 4, complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 6**    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 15454, the ACT/STBY LED is illuminated.

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

**Step 7**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the standby cross-connect card.

**Step 8**    If the card reporting the alarm is a traffic card, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-166.

**Step 9**    If the alarm does not clear after the cross-connect card side switch, complete the "Reset a Traffic Card in CTC" procedure on page 2-169 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 10**    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 15454, the ACT/STBY LED is illuminated.

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

**Step 11**    If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the traffic line card.

**Step 12**    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).

## 2.6.229  SWTOPRI

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

**Note**    SWTOPRI is an informational condition. It does not require troubleshooting.

## 2.6.230  SWTOSEC

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

### Procedure:  Clear the SWTOSEC Condition

**Step 1**    To clear the condition, clear alarms related to failures of the primary source, such as SYNCPRI, page 2-153.

**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).

## 2.6.231  SWTOTHIRD

- Not Alarmed (NA), Non-Service Affecting (NSA)

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

### Procedure:  Clear the SWTOTHIRD Condition

**Step 1**    To clear the condition, clear alarms related to failures of the primary source, such as SYNCPRI, page 2-153, or SYNCSEC, page 2-154.

**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).

## 2.6.232  SYNC-FREQ

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Synchronization Reference Frequency Out Of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

### 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 it falls within the proper frequency:

For specific procedures to use the test set equipment, consult the manufacturer. For BITS, the proper timing frequency range is approximately -15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately -16 PPM to 16 PPM.

**Step 2**  If the reference source frequency is not outside of bounds, complete the "Physically Replace a Card" procedure on page 2-169 for the TCC+/TCC2 card.

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

> **Note**  It takes up to 30 minutes for the active TCC+/TCC2 to transfer the system software to the newly installed TCC+/TCC2. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the TCC+/TCC2 flash fail and then the active/standby LED flashes. When the transfer completes, the TCC+/TCC2 reboots and goes into standby mode after approximately three minutes.

**Step 3**  If the SYNC-FREQ condition continues to report after replacing the TCC+/TCC2 card, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.6.233  SYNCPRI

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers SWTOSEC, page 2-152.

### Procedure:  Clear the SYNCPRI Alarm

**Step 1**  In the 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 2-101.

**Step 4**    If the primary reference clock is an incoming port on the ONS 15454, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

**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).

# 2.6.234  SYNCSEC

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to the third timing source also triggers SWTOTHIRD, page 2-152.

## Procedure:  Clear the SYNCSEC Alarm

**Step 1**    In the 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 2-101.

**Step 4**    Verify that the BITS clock is operating properly.

**Step 5**    If the secondary timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

**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).

# 2.6.235  SYNCTHIRD

- Minor (MN), Non-Service Affecting (NSA)

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC+/TCC2 card might have failed. The ONS 15454 often reports either FRNGSYNC, page 2-82, or HLDOVRSYNC, page 2-87, after a SYNCTHIRD alarm.

⚠

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

## Procedure:  Clear the SYNCTHIRD Alarm

**Step 1**    In node view, click the **Provisioning > Timing** tabs.

**Step 2**    Verify that the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 3**    If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-101.

**Step 4**    If the third timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

**Step 5**    If the third timing source uses the internal ONS 15454 timing, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 6**    If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

## 2.6.236  SYSBOOT

- Major (MJ), Service Affecting (SA)

The System Reboot alarm indicates that new software is booting on the TCC+/TCC2 card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If it does not clear, log onto http://www.cisco.com/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.

## 2.6.237  TIM-P

- Critical (CR), Service Affecting (SA) for STSTERM
- Minor (MN), Non-Service Affecting (NSA) for STSMON

The TIM Path alarm (TIM-P) is raised when the expected SONET path trace string does not match the received path trace string.

The alarm is raised on an incoming SONET span card in the following sequence:

- A signal error occurs on a DS-1 or DS-3 electrical signal;
- The electrical card reports the error to the TCC2;
- The TCC2 determines that the error is on the SONET overhead instead of the electrical signal itself, and raises the alarm against the receiving SONET port.

Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur. In manual mode at the Path Trace window, type the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or a new, incorrect value has been entered in the Current Transmit String field. This procedure applies to either situation.

TIM-P also occurs on a port that has previously been operating without alarms if DS-3 cables or optical fibers connecting the ports are switched or removed. TIM-P is usually accompanied by other alarms, such as the LOS (OC-N) alarm (see page 2-105), the UNEQ-P alarm (see page 2-159), or the PLM-P alarm (see page 2-128). 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** 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).

# 2.6.238  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 G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as AIS-P, page 2-22; LOP-P, page 2-98; PDI-P, page 2-126, or UNEQ-P, page 2-159, exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 Ethernet port is administratively disabled or it is reporting CARLOSS (G-Series), page 2-39, the C2 byte in the SONET path overhead indicates a PDI-P alarm. This, 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 G1000-4 port or the far-end G1000-4 port to which it is mapped.

## Procedure:  Clear the TPTFAIL (G-Series) Alarm

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

**Step 2**   If no alarms are reported by the OC-N card, or if a PDI-P alarm is reported, the problem might be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

**Step 3**   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.6.239  TPTFAIL (ML-Series)

- Major (MJ), Service Affecting (SA)

The TPT Layer Failure alarm for the ML-series Ethernet (traffic) cards indicates a break in the end-to-end POS link integrity feature of the ML-series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on either the SONET path, the remote POS port, or a misconfiguration of the POS port which prevents the complete end-to-end POS path from working. If any SONET path alarms such as AIS-P, page 2-22; LOP-P, page 2-98; PDI-P, page 2-126, or UNEQ-P, page 2-159, exist on the circuit used by the POS port, the affected port might report a TPTFAIL alarm. If the far-end ML-series POS port is administratively disabled, it inserts an AIS-P condition that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the IOS CLI level, the misconfiguration will cause the port to go down and report TPTFAIL.

## Procedure:  Clear the TPTFAIL (ML-Series) Alarm

**Step 1**   If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.

**Step 2**   If PLM-P, page 2-128, is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.

**Step 3**   If a PDI-P alarm is the only one reported against the POS port circuit and the circuit is terminated by a G-series card, verify whether CARLOSS (G-Series), page 39, is reported against the G-series card and if so, complete the "Clear the CARLOSS (G-Series) Alarm" procedure on page 2-40.

**Step 4**   If an AIS-P condition, an LOP-P alarm, or an UNEQ-P alarm is present, clear those alarms using the procedures in those sections.

**Step 5**  If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.240  TRMT

- Major (MJ), Service Affecting (SA)

A Missing Transmitter alarm occurs when there is a transmit failure on the DS-1 card because of an internal hardware failure. The card must be replaced.

### Procedure:  Clear the TRMT Alarm

**Step 1**  Complete the "Physically Replace a Card" procedure on page 2-169 for the reporting DS-1 card.

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

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

**Step 2**  If the alarm does not clear, call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).

## 2.6.241  TRMT-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector connects to a DS-1 card instead of a DS-3 card.

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

### Procedure:  Clear the TRMT-MISS Alarm

**Step 1**  Verify that the device attached to the DS-1 port is operational.

**Step 2**  If the device is operational, verify that the cabling is securely connected.

**Step 3**  If the cabling is secure, verify that the pinouts are correct.

**Step 4**     If the pinouts are correct, replace the transmit cable.

**Step 5**     If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

## 2.6.242  UNC-WORD

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Uncorrected Forward Error Correction (FEC) Word condition indicates that forward error correction (FEC), which is used to lower signal to noise ratio by 7dB to 8dB, could not correct the frame sufficiently.

### Procedure:  Clear the UNC-WORD Condition

**Step 1**     Complete the "Clear the SD Condition" procedure on page 2-140.

**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).

## 2.6.243  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.

**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, page 2-22, is reported on the terminating cards. These alarms clear when the circuit carries a signal.

**Caution**     Deleting a circuit affects traffic.

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

### Procedure:  Clear the UNEQ-P Alarm

**Step 1**     In the 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):

> **Note**   The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

    **a.**   Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-167.

    **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 whether the circuits are complete:

    **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 2-167.

**Step 10**   Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide*.

**Step 11**   Log back in and verify that all circuits terminating in the reporting card are active:

    **a.**   Click the **Circuits** tab.

    **b.**   Verify that the **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 15454 Procedure Guide*.

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

> **Warning**   **Invisible laser radiation 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.**

**Step 13**   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the OC-N and DS-N cards.

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

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

**Step 14**    If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

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

**Warning**    **Invisible laser radiation 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 15454. Plug the wristband cable into the ESD jack located at the lower-right outside edge of the shelf assembly.

## Procedure:  Clear the UNEQ-V Alarm

**Step 1**    Complete the "Clear the UNEQ-P Alarm" procedure on page 2-159.

**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).

## 2.6.245  WKSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Working Switched To Protection condition occurs when a line experiences an LOS (OC-N), page 2-105; an SF, page 2-141, or an SD, page 2-139.

### Procedure:  Clear the WKSWPR Condition

**Step 1**    Complete the "Clear the LOS (OC-N) Alarm" 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 to report a service-affecting problem (1-800-553-2447).

## 2.6.246  WTR

- Not Alarmed (NA), Non-Service Affecting (NSA)

The Wait To Restore condition occurs when WKSWPR, page 2-162, 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]

**Note**    WTR is an informational condition. It does not require troubleshooting.

## 2.6.247  WVL-MISMATCH

- Major (MJ), Service Affecting (SA)

The Equipment Wavelength Mismatch alarm applies to the TXP and MXP cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

### Procedure: Clear the WVL-MISMATCH alarm

**Step 1**    In node view, double-click the TXP or MXP card to display the card view.

**Step 2**    Click the **Provisioning > Card** tabs.

**Step 3**    In the Wavelength field, view the provisioned card wavelength.

**Step 4**    If you have access to the site, compare the wavelength listed on the card faceplate with the provisioned wavelength. If you are remote, compare this wavelength with the card identification in the inventory:

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

    **b.**    Locate the slot where the TXP or MXP card is installed and view the card wavelength in the name.

**Step 5**    If the card was provisioned for the wrong wavelength, double-click the card in the node view to display the card view.

**Step 6**    Click the **Provisioning > Card** tabs.

**Step 7**    In the Wavelength field, click the pull-down menu and choose the correct wavelength.

**Step 8** Click **Apply**.

**Step 9** If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

# 2.7 DS3-12 E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M13, or C-bit. The choice of framing format determines the line alarms that the DS3-12E card reports. The following table lists the line alarms reported under each format.

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

*Table 2-8    DS3-12E Line Alarms*

| Alarm | UNFRAMED | M13 | CBIT |
|---|---|---|---|
| LOS | ◆ | ◆ | ◆ |
| AIS | ◆ | ◆ | ◆ |
| LOF | ○ | ◆ | ◆ |
| IDLE | ○ | ◆ | ◆ |
| RAI | ○ | ◆ | ◆ |
| Terminal Lpbk | ◆ | ◆ | ◆ |
| Facility Lpbk | ◆ | ◆ | ◆ |
| FE Lpbk | ○ | ○ | ◆ |
| FE Common Equipment Failure | ○ | ○ | ◆ |
| FE Equipment Failure-SA | ○ | ○ | ◆ |
| FE LOS | ○ | ○ | ◆ |
| FE LOF | ○ | ○ | ◆ |
| FE AIS | ○ | ○ | ◆ |
| FE IDLE | ○ | ○ | ◆ |
| FE Equipment Failure-NSA | ○ | ○ | ◆ |

# 2.8  Common Procedures in Alarm Troubleshooting

This section gives common procedures that are frequently used when troubleshooting alarms. For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 Procedure Guide*.

## Procedure:  Identify a Ring ID or Node ID Number

**Step 1**  Log into a node on the network. If you are already logged in, go to Step 2.

**Step 2**  In the 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 the 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 the 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, continue with Step 2.

**Step 2**    In 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, continue with Step 2.

**Step 2**    In the node view, click the **Provisioning > DCC/GCC** 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, continue with Step 2.

**Step 2**    In the node view, click the **Maintenance > BLSR** tabs.

**Step 3**    Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.

**Step 4**    Choose **LOCKOUT 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, continue with Step 2.

**Step 2**    In the node view, click the **Maintenance > BLSR** tabs.

**Step 3**    Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.

**Step 4**    Choose **CLEAR** and click **Apply**.

**Step 5**    Click **OK** on the BLSR Operations dialog box.

## Procedure:  Clear a Path Protection Lock Out

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    In the node view, click **View > Go to Network View**.

**Step 3**    Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

**Step 4**    In the Circuits on Span dialog box, choose **CLEAR** from the Perform UPSR Span Switching pull-down menu to remove a previously set switch command. Click **Apply**.

**Step 5**    In the Confirm UPSR Switch dialog box, click **Yes**.

**Step 6**    In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the switch state for all path protection circuits is CLEAR.

## 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, continue with Step 2.

**Step 2**    Display the node view.

**Step 3**    In the node view, click the **Maintenance > Protection** tabs.

**Step 4**    Double-click the protection group that contains the reporting card.

**Step 5**    Click the Working or active card of the selected groups.

**Step 6**    Click **Switch** and **Yes** in the Confirmation dialog box.

## Procedure:  Side Switch the Active and Standby Cross-Connect Cards

⚠

**Caution**    The cross-connect card side switch is traffic-affecting.

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    Display the node view.

**Step 3**    Determine the active or standby cross-connect card.

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

✎

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

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

**Step 5**    Click **Switch**.

**Step 6**    Click **Yes** in the Confirm Switch dialog box.

## Procedure:  Clear an External Switching Command

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    In the 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, continue with Step 2.

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

**Step 3**    Click the circuit row to highlight it and click **Delete**.

**Step 4**    Click **Yes** 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, continue with Step 2.

**Step 2**    Double-click the reporting card in CTC to display the card view.

**Step 3**    Click the **Maintenance** tab.

**Step 4**    In the Loopback Type column, determine whether any port row shows a state other than None.

**Step 5**    If a row contains another state besides None, click in the column cell to display the pull-down menu and select None.

**Step 6**    In the State column, determine whether any port row shows a state other than IS.

**Step 7**    If a row shows a state other than IS, click in the column cell to display the pull-down menu and select **IS**.

**Step 8**    Click **Apply**.

## Procedure:  Reset Active TCC+/TCC2 Card and Activate Standby Card

⚠️

**Caution**    The TCC+ or TCC2 card reset can be traffic-affecting.

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    Identify the active TCC+/TCC2 card.

If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+/TCC2 is green. The ACT/STBLY LED of the standby TCC+/TCC2 is amber.

**Step 3**    Right-click the active TCC+/TCC2 card in CTC.

**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.

**Step 6**    Verify that the reset is complete and error-free.

Double-click the node and ensure that the reset TCC+/TCC2 card is in standby mode and that the other TCC+/TCC2 card is active.

- If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+/TCC2 is green. The ACT/STBLY LED of the standby TCC+/TCC2 is amber.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the active TCC+/TCC2 ACT/STBY LED is green, and the LED of the standby TCC+/TCC2 is amber.


## Procedure:  Remove and Reinsert (Reseat) the Standby TCC+/TCC2

⚠️

**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).

⚠️

**Caution**    The TCC+ or TCC2 card reseat can be traffic-affecting.

✎

**Note**    Before you reset the TCC+ or TCC2, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    Ensure that the TCC+/TCC2 you want to reset is in standby mode. On the TCC+/TCC2 card, the ACT/STBY (Active/Standby) LED is amber when the TCC+/TCC2 is in standby mode.

**Step 3**    When the TCC+/TCC2 is in standby mode, unlatch both the top and bottom ejector levers on the TCC+/TCC2 card.

**Step 4**    Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

**Step 5**    Wait 30 seconds. Reinsert the card and close the ejector levers.

> **Note**    The TCC+/TCC2 will take several minutes to reboot and will display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about LED behavior during TCC+/TCC2 card reboots.

## Procedure:  Reset a Traffic Card in CTC

**Step 1**    Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2**    In node view, position the cursor over the multispeed slot (Slots 1 to 4 and 14 to 17) or high-speed slot (Slots 5,6 and 12 and 13) 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, continue with Step 2.

**Step 2**    In the node view, double-click the card reporting the alarm to display the card view.

**Step 3**    Click the **Provisioning > Line** tabs.

**Step 4**    Under the **SD BER** (or **SF BER**) column on the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

**Step 5**    If the entry is consistent with the original provisioning, go back to your original procedure.

**Step 6**    If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

**Step 7**    Click **Apply**.

## 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

**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 15454.

**Step 3**    Close the retractable handles.

# Replace Hardware

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

This chapter provides procedures for replacing Cisco ONS 15454 hardware.

1. Replace an In-Service Cross-Connect Card, page 3-1—Complete this procedure to replace an in-service cross-connect card.

2. Replace the Air Filter, page 3-5—Complete this procedure to replace a reusable or disposable air filter.

3. Determine Fan-Tray and AIP Replacement Compatibility, page 3-9—Complete this procedure to verify replacement hardware compatibility.

4. Replace the Fan-Tray Assembly, page 3-11—Complete this procedure to replace the fan-tray assembly.

5. Replace the Alarm Interface Panel, page 3-12—Complete this procedure to replace the alarm interface panel (AIP).

6. Replace an Electrical Interface Assembly, page 3-17—Complete this procedure to replace the electrical interface assembly (EIA).

7. Replace the Small-Formfactor Pluggable Connector, page 3-18—Complete this procedure as needed to replace the small-form pluggable (SFP) connector used with ML-Series Ethernet cards.

## 3.1  Replace an In-Service Cross-Connect Card

⚠
**Warning** **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

⚠

**Caution**    Removing any active card from the ONS 15454 can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, follow the steps below to switch the XC/XCVT/XC10G card to standby prior to removing the card from the node.

✎

**Note**    An improper removal (IMPROPRMVL) alarm is raised when a card reseat is performed, unless the card is first deleted in CTC. The alarm will clear after the card replacement is complete.

In a BLSR, path protection configuration, or 1+1 configuration, pulling the active cross-connect card (XC/XCVT/XC10G) without a lock out might cause circuits to switch. Therefore, you must inhibit protection switching before replacing the in-service cross-connect card.

**Step 1**    Log into the node where you will replace the card. For login procedures, see the *Cisco ONS 15454 Procedure Guide*.

**Step 2**    Ensure the working span is active on both local and remote nodes. The purpose of verifying the active span is to know which one to lock out:

   **a.**    In node view, click the **Maintenance > BLSR** tabs.

   **b.**    Locate the applicable span.

   In the West Line and East Line columns, the working/active span is identified by (Work/Act).

**Step 3**    Make sure that no alarm filters are applied. Ensure the working span is carrying error-free traffic (no SD or SF alarms present). Display the network view and click the **Alarms** tab to display alarms.

**Step 4**    Lock out or switch the protection span according to the network topology. To lock out a BLSR, go to Step 5. To lock out a protection span in a 1+1 protection scheme, go to Step 6. To switch path protection configuration traffic, go to Step 7.

**Step 5**    Lock out the protection span in a BLSR protection scheme:

   **a.**    In node view, click the **Provisioning > BLSR** tabs.

   **b.**    Choose the BLSR and click **Edit**.

💡

**Tip**    To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

   **c.**    To lock out a west span:

   •    Right-click any BLSR node west channel (port) and choose **Set West Protection Operation**.

✎

**Note**    For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. You can right-click either working port.

   •    In the Set West Protection Operation dialog box, choose **LOCKOUT SPAN** from the pull-down menu. Click **OK**.

   •    In the Confirm BLSR Operation dialog box, click **Yes**. An "L" indicating the lock out appears on the selected channel (port) where you created the lock out.

- Lock outs generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

   **d.**  To lock out an east span:

- Right-click the node's east channel (port) and choose **Set East Protection Operation**.

- In the Set East Protection Operation dialog box, choose **LOCKOUT SPAN** from the pull-down menu. Click **OK**.

- In the Confirm BLSR Operation dialog box, click **Yes**. An "L" indicating the lock out appears on the selected channel (port) where you invoked the protection switch.

- Lock outs generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

- From the File menu, choose **Close**.

**Step 6**   To lock out a protection span in a 1+1 protection scheme:

   **a.**  In node view, click the **Maintenance > Protection** tabs.

   **b.**  Under Protection Groups, click the protection group that contains the card you want to lock out.

   **c.**  Under Selected Group, click the card you want to lock traffic out of.

   **d.**  From Inhibit Switching, click **Lock Out**.

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

   The lock out has been applied and traffic is switched to the opposite card.

> **Note**   Provisioning a lock out causes a LOCKOUT-REQ or an FE-LOCKOUT condition to be raised on CTC. Clearing the lock out switch request clears these conditions; they are informational only.

**Step 7**   To Force switch traffic in a path protection configuration protection scheme:

- In node view, choose **Go to Network View**.

- Right-click the span where you want to switch path protection configuration traffic away. Choose **Circuits** from the shortcut menu.

- In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

- In the Confirm UPSR Switch dialog box, click **Yes**.

- In the Protection Switch Result dialog box, click **OK**.

   In the Circuits on Span window, the Switch State for all circuits is Force.

> **Note**   A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the Force switch; it is informational only.

**Step 8**   When the protection span has been locked out, determine the active cross-connect card (XC/XCVT/XC10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

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

**Step 9**  Switch the active cross-connect card (XC/XCVT/XC10G) to standby:

    **a.**  In the node view, click the **Maintenance > XC Cards** tabs.

    **b.**  Under Cross Connect Cards, choose **Switch**.

    **c.**  Click **Yes** on the Confirm Switch dialog box.

> **Note**  After the active XC/XCVT/XC10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

**Step 10**  Physically remove the new standby cross-connect card (XC/XCVT/XC10G) from the ONS 15454.

**Step 11**  Insert the replacement cross-connect card (XC/XCVT/XC10G) into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

**Step 12**  Release the protection lock out(s) applied in Step 4:

    **a.**  Release the lock out of the protection span in a BLSR protection scheme:

    •  In node view, click the **Provisioning > BLSR** tabs.

    •  Choose the BLSR and click **Edit**.

> **Tip**  To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

    •  Right-click the BLSR node channel (port) where the lock out will be cleared and choose **Set West Protection Operation or Set East Protection Operation**.

    •  In the dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

    •  In the Confirm BLSR Operation dialog box, click **Yes**. The "L" indicating the lock out is removed from the network view map.

    •  From the File menu, choose **Close**.

    **b.**  Release the lock out of the protection span in a 1+1 protection scheme:

    •  In node view, click the **Maintenance > Protection** tabs.

    •  Under Protection Groups, click the protection group that contains the card you want to clear.

    •  Under Selected Group, click the card you want to clear.

    •  From Inhibit Switching, click **Unlock**.

    •  Click **Yes** on the confirmation dialog box.

    **c.**  Clear the Force switch for the path protection configuration protection scheme:

    •  In node view, choose **Go to Network View**.

    •  Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

    •  In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.

    •  In the Confirm UPSR Switch dialog box, click **Yes**.

    •  In the Protection Switch Result dialog box, click **OK**.

    In the Circuits on Span window, the Switch State for all path protection circuits is CLEAR.

The lock out is cleared.

# 3.2  Replace the Air Filter

Inspect the air filters every 30 days and clean as needed.

## 3.2.1  Inspect, Clean, and Replace the Reusable Air Filter

You need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

**Warning**    **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

**Step 1**    Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.

**Step 2**    If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that may have collected on the filter and proceed to Step 3. Figure 3-1 illustrates a reusable fan-tray air filter in an external filter bracket. If the filter is installed beneath the fan tray and not in the external filter brackets:

 **a.**  Open the front door of the shelf assembly. If it is already open or the shelf assembly does not have a front door, continue with Step 3.

  •  Open the front door lock.

   The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

  •  Press the door button to release the latch.

  •  Swing the door open.

 **b.**  Remove the front door (optional). If you do not want to remove the door, proceed to Step 3:

  •  Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

  •  Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

  •  Secure the dangling end of the ground strap to the door or chassis with tape.

*Figure 3-1    A Reusable Fan-Tray Air Filter in an External Filter Bracket (Front Door Removed)*
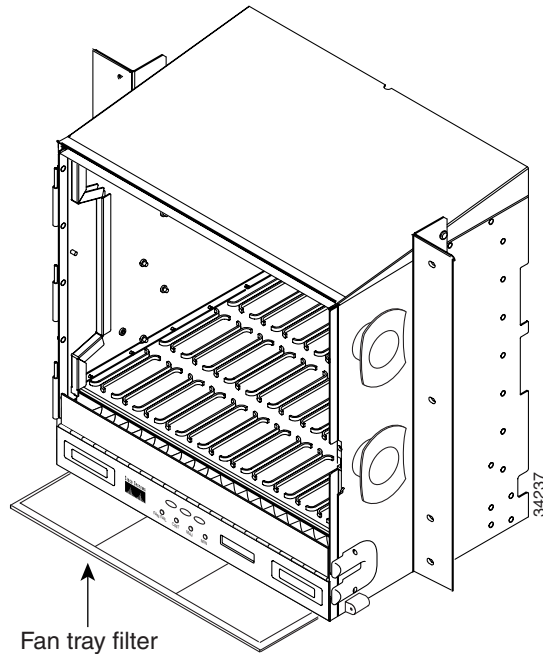


Fan tray filter

**Step 3**    Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 4**    Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.

**Step 5**    When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

**Step 6**    Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that may have collected on the filter.

**Step 7**    Visually inspect the air filter material for dirt and dust.

**Step 8**    If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.

**Note**    Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

**Step 9**    If you washed the filter, allow it to completely air dry for at least eight hours.

**Caution**    Do not put a damp filter back in the ONS 15454.

**a.**    If the air filter is installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

**b.**    If the filter is installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

⚠

**Caution**    If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

✎

**Note**    On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

**Step 10**    To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

**Step 11**    Rotate the retractable handles back into their compartments.

**Step 12**    If you replace the door, also reattach the ground strap.


## 3.2.2  Inspect and Replace the Disposable Air Filter

The disposable air filter is installed beneath the fan-tray assembly only, so you must remove the fan-tray assembly to inspect and replace the disposable air filter.

**Step 1**    Verify that you are replacing a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. NEBS 3E and earlier versions of the ONS 15454 use a disposable air filter.

**Step 2**    Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with Step 4.

   **a.**    Open the front door lock.

   The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

   **b.**    Press the door button to release the latch.

   **c.**    Swing the door open.

**Step 3**    Remove the front door (optional). If you do not want to remove the door, proceed to Step 4.

   **a.**    Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

   **b.**    Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

   **c.**    Secure the dangling end of the ground strap to the door or chassis with tape.

**Step 4**    Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 5**    Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.

**Step 6**    When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 3-2).

*Figure 3-2    Inserting or Removing the Fan-Tray Assembly (Front Door Removed)*



Fan tray
assembly

Fan tray filter

Small engraved
direction arrow

71527
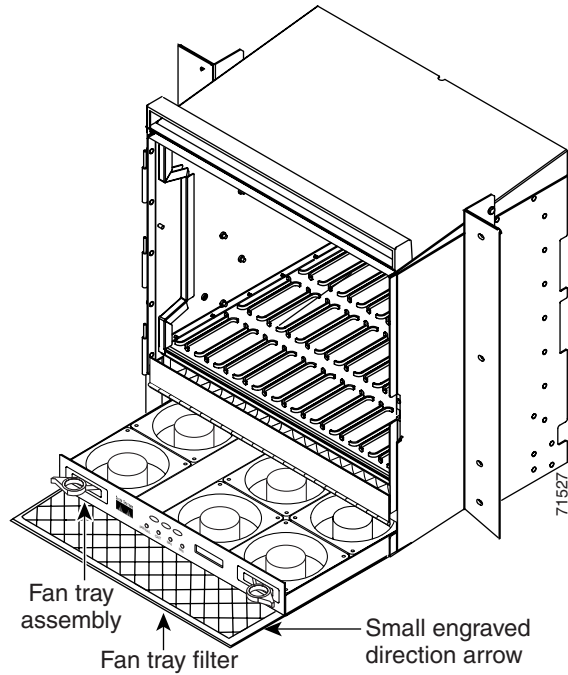
**Step 7**    Gently remove the air filter from the shelf assembly (Figure 3-3). Be careful not to dislodge any dust that may have collected on the filter.

**Step 8**    Visually inspect the white filter material for dirt and dust.

**Step 9**    If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter by sliding the filter into the bottom of the shelf assembly. Make sure that the front of the filter is flush with the front of the shelf assembly and that the air flow indicators on the filter point upwards.

*Figure 3-3    Inserting or Removing a Disposable Fan-Tray Air Filter (Front Door Removed)*



Fan tray filter
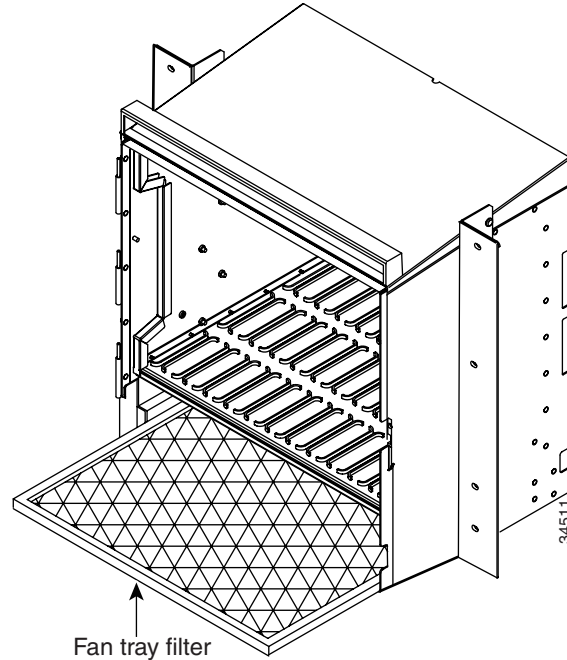
**Step 10**    Slide the fan-tray assembly into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

**Step 11**    To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

**Step 12**    Rotate the retractable handles back into their compartments.

**Step 13**    If you replace the door, also reattach the group strap.

# 3.3  Determine Fan-Tray and AIP Replacement Compatibility

⚠️

**Caution**    The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.

**Note**    The 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC10G, OC-192, and OC-48AS cards.

**Note**    The 5A AIP (73-7665-XX) is required when installing the 15454-FTA3 fan-tray assembly.

**Step 1** Review Table 3-1 to ensure you have compatible components when replacing the fan-tray assembly or the AIP and note the alarms that will occur when an incompatibility occurs.

✎

**Note** If you need to determine the hardware that has been installed on a node, click the inventory tab in node view.

*Table 3-1    Incompatibility Alarms*

| Shelf Assembly [1] | Fan Tray[2] | AIP[3] | 10G Cards[4] | Ethernet Cards[5] | Alarms |
|---|---|---|---|---|---|
| — | — | No fuse | — | — | MEA on AIP |
| NEBS3E or NEBS3 | 2A | 2A | No | — | None |
| NEBS3E or NEBS3 | 2A | 2A | Yes | — | MEA on 10G |
| NEBS3E or NEBS3 | 2A | 5A | No | — | None |
| NEBS3E or NEBS3 | 2A | 5A | Yes | — | MEA on 10G |
| ANSI | 2A | 2A | No | — | None |
| ANSI | 2A | 2A | Yes | 2.5G compatible | MEA on fan tray, AIP, Ethernet |
| ANSI | 2A | 2A | Yes | 10G compatible | MEA on fan tray, AIP |
| ANSI | 2A | 5A | No | Either | None |
| ANSI | 2A | 5A | Yes | 2.5G compatible | MEA on fan tray, Ethernet |
| ANSI | 2A | 5A | Yes | 10G compatible | MEA on fan tray |
| ANSI | 5A | 2A | No | Either | MEA on AIP |
| ANSI | 5A | 2A | Yes | 2.5G compatible | MEA on AIP, Ethernet |
| ANSI | 5A | 2A | Yes | 10G compatible | MEA on AIP |
| ANSI | 5A | 5A | No | Either | None |
| ANSI | 5A | 5A | Yes | Either | None |

1.  15454-SA-ANSI (P/N: 800-19857-01) = ONS 15454 Release 3.1 and later shelf assembly,
    15454-SA-NEBS3E (P/N: 800-07149-xx) or 15454-SA-NEBS3 (P/N: 800-06741-xx) = shelf assemblies released before
    ONS 15454 Release 3.1

2.  5A Fan Tray = 15454-FTA3 (P/N: 800-19858-xx) or 15454-FTA3-T (P/N: 800-21448-xx),
    2A Fan Tray = 15454-FTA2 (P/Ns: 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx)

3.  5A AIP (P/N: 73-7665-01), 2A AIP (P/N: 73-5262-01)

4.  10G cards = XC-10G, OC-192, OC-48AS

5.  2.5G compatible Ethernet cards = E1000-T, E1000-2, E1000T-G, E10002-G, G1000-4, G1K-4
    10G compatible Ethernet cards = E1000T-G, E10002-G, G1000-4, G1K-4, ML100T-12, ML1000-2

**Step 2** See the "Replace the Fan-Tray Assembly" section on page 3-11 to replace the fan-tray assembly or the "Replace the Alarm Interface Panel" section on page 3-12 to replace the AIP.

# 3.4  Replace the Fan-Tray Assembly

⚠

**Caution**     The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a non-compatible shelf assembly.

⚠

**Caution**     Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

✎

**Note**     The 15454-SA-ANSI shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 XC-10G, OC-192, and OC-48 any slot (AS) cards.

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

**Step 1**     Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with Step 3.

  **a.**   Open the front door lock.

  The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

  **b.**   Press the door button to release the latch.

  **c.**   Swing the door open.

**Step 2**     Remove the front door (optional). If you do not want to remove the door, proceed to Step 3.

  **a.**   Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

  **b.**   Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

  **c.**   Secure the dangling end of the ground strap to the door or chassis with tape.

**Step 3**     Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 4**     Fold out the retractable handles at the outside edges of the fan tray.

**Step 5**     Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.

**Step 6**     When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly. Figure 3-4 shows the location of the fan tray.

*Figure 3-4     Removing or Replacing the Fan-Tray Assembly (Front Door Removed)*



LCD     Fan tray
assembly
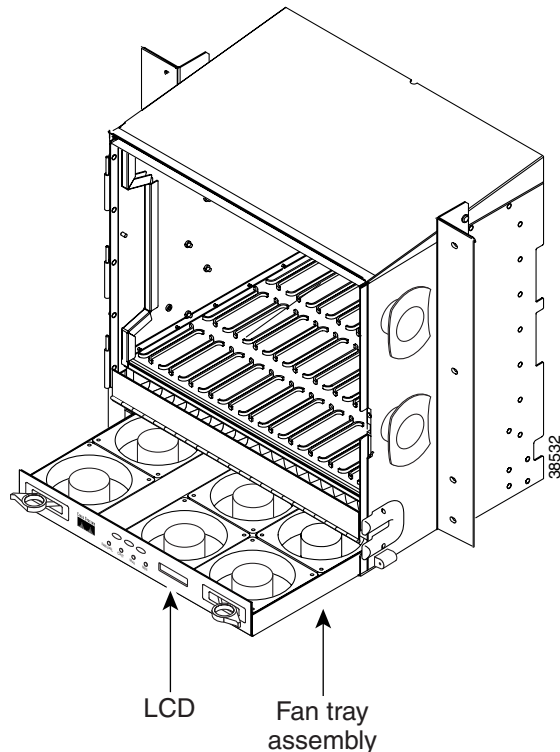
**Step 7**   If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the "Replace the Air Filter" section on page 3-5.

**Step 8**   Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

**Step 9**   To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

**Step 10**   If you replace the door, also reattach the ground strap.

# 3.5  Replace the Alarm Interface Panel

⚠

**Caution**   Do not use a 2A AIP with a 5A fan-tray assembly; doing so will cause a blown fuse on the AIP.

⚠

**Caution**   If any nodes in an Ethernet circuit are not using Software Release 4.0, there is a risk of Ethernet traffic disruptions. Contact the Cisco Technical Assistance Center (TAC) at 800-553-2447 when prompted to do so in the procedure.

⚠️

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

✎

**Note**  Perform this procedure during a maintenance window. Resetting the active TCC+/TCC2 card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC+/TCC2 card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software Release 4.0.

⚠️

**Caution**  Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco Technical Assistance Center (TAC) at 800-553-2447.

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to 4.0 will be affected.

You need a #2 Phillips screwdriver.

**Step 1**  Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

   **d.**  In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.

   **e.**  If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.

**Step 2**  Record the MAC address of the old AIP:

   **a.**  Log into the node where you will replace the AIP. For login procedures, see the *Cisco ONS 15454 Procedure Guide*.

   **b.**  In node view, click the **Provisioning > Network** tabs.

   **c.**  Record the MAC address shown in the General tab (Figure 3-5).

*Figure 3-5    Find the MAC Address*
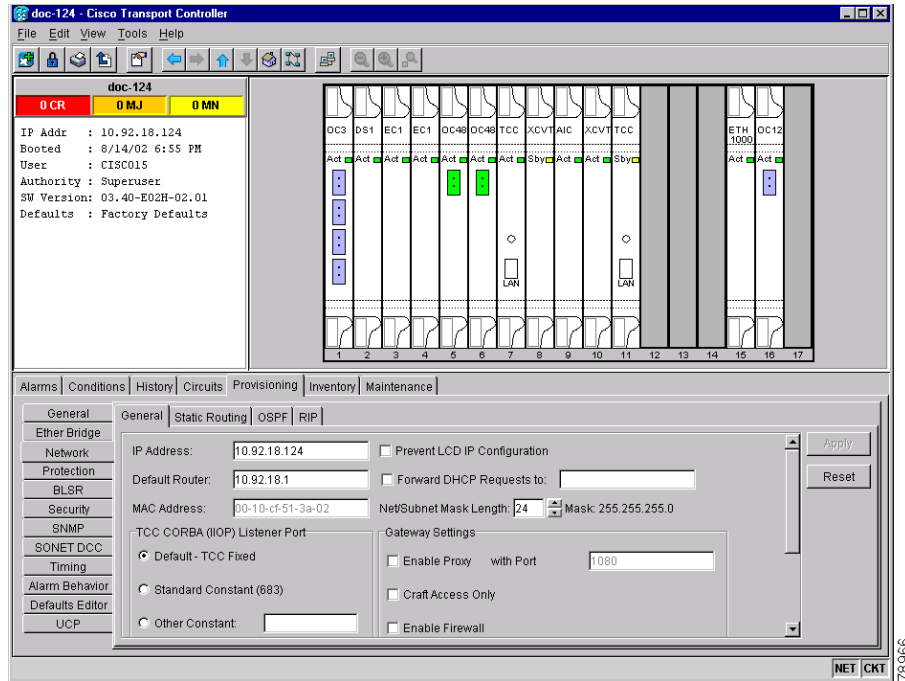


**Step 3** Call Cisco TAC at 800-553-3227 for assistance in replacing the AIP and maintaining the original MAC address.

**Step 4** Unscrew the five screws that hold the lower backplane cover in place (Figure 3-6).

**Step 5** Grip the lower backplane cover and gently pull it away from the backplane.

*Figure 3-6    Lower Backplane Cover*



Retaining screws
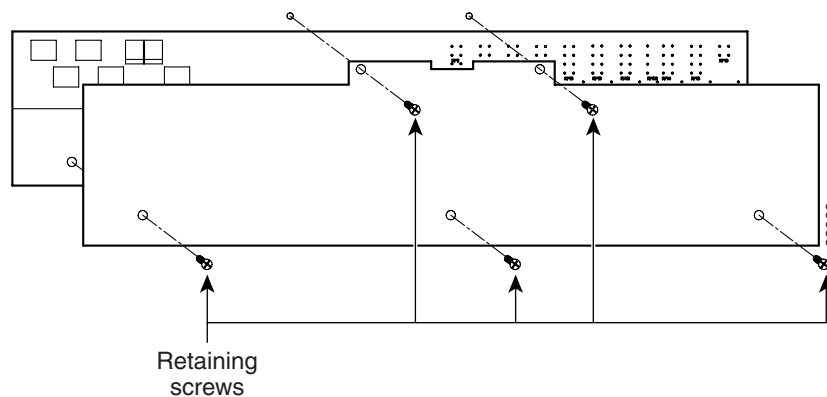
**Step 6** Unscrew the two screws that hold the AIP cover in place.

**Step 7** Grip the cover and gently pull away from the backplane.

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

**Step 8**   Grip the AIP and gently pull it away from the backplane.

**Step 9**   Disconnect the fan-tray assembly power cable from the AIP.

**Step 10**  Set the old AIP aside for return to Cisco.

⚠
**Caution**   The type of shelf the AIP resides in will determine the version of AIP that will replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) currently uses the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and lower currently use the 2A AIP (P/N: 73-5262-01).

⚠
**Caution**   Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI shelf (P/N: 800-19857); doing so will cause a blown fuse on the AIP.

**Step 11**  Attach the fan-tray assembly power cable to the new AIP.

**Step 12**  Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

**Step 13**  Replace the AIP cover over the AIP and secure the cover with the two screws.

**Step 14**  Replace the lower backplane cover and secure the cover with the five screws.

**Step 15**  In node view, click the **Provisioning > Network** tabs.

⚠
**Caution**   Cisco recommends TCC+/TCC2 resets be performed in a maintenance window to avoid any potential service disruptions.

**Step 16**  Reset the standby TCC+/TCC2 card:

   **a.**  Right-click the standby TCC+/TCC2 card and choose **Reset Card**.

   **b.**  Click **Yes** on the Resetting Card dialog box. As the card resets, a loading (Ldg) indication will appear on the card in CTC.

✎
**Note**   The reset will take approximately five minutes. Do not perform any other steps until the reset is complete.

**Step 17**  Reset the active TCC+/TCC2 card:

   **a.**  Right click the active TCC+/TCC2 card and choose **Reset Card**.

   **b.**  Click **Yes** on the Resetting Card dialog box. As the card resets, a Ldg indication will appear on the card in CTC.

✎
**Note**   The reset will take approximately five minutes and CTC will lose its connection with the node.

**Step 18**  From the **File** pull-down menu choose **Exit** to exit the CTC session.

**Step 19**  Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes pull-down menu.

**Step 20**  Record the new MAC address:

   **a.**  In node view, click the **Provisioning > Network** tabs.

**b.** Record the MAC address shown in the General tab.

**Step 21** In node view, click the **Circuits** tab. Note that all circuits listed are in an INCOMPLETE state.

**Step 22** In node view, choose **Repair Circuits** from the **Tools** pull-down menu. The Circuit Repair dialog box is displayed.

**Step 23** Read the instructions in the Circuit Repair dialog box (Figure 3-7). If all the steps in the dialog box have been completed, click **Next>**. Ensure you have the old and new MAC addresses.

*Figure 3-7     Repairing Circuits*
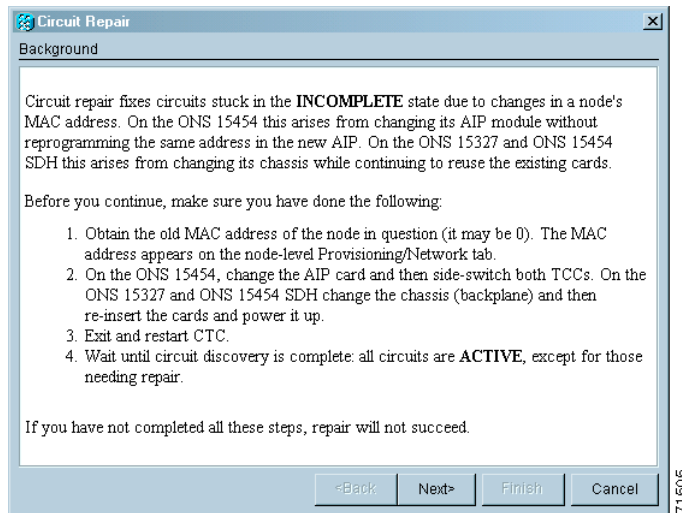


**Step 24** The Node MAC Addresses dialog box displays (Figure 3-8):

**a.** From the Node pull-down menu, choose the name of the node where you replaced the AIP.

**b.** In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.

**c.** Click **Next**.

*Figure 3-8     Recording the Old MAC Address Before Replacing the AIP*
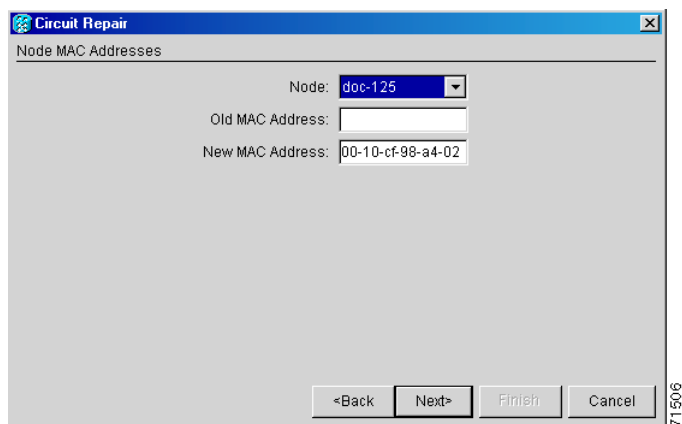


**Step 25** The Repair Circuits dialog box displays (Figure 3-9). Read the information in the dialog box and click **Finish**.

*Figure 3-9    Circuit Repair Information*
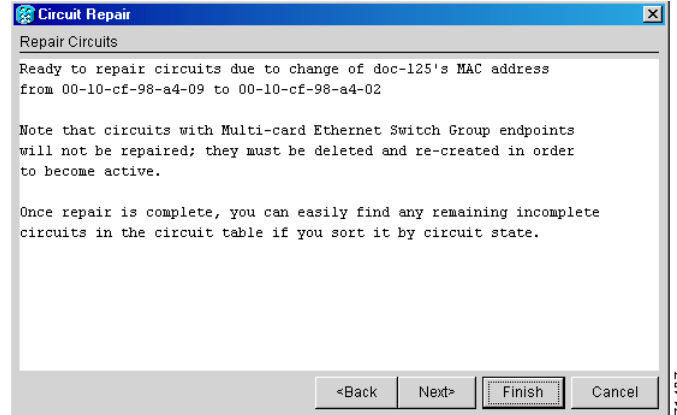


> **Note**  The CTC session will freeze until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

When the circuit repair is complete, the Circuits Repaired dialog box will display.

**Step 26**    Click **OK**.

**Step 27**    In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are in an ACTIVE state. If all circuits listed are not in an ACTIVE state, call the Cisco Technical Assistance Center TAC at 800-553-2447 to open a Return Material Authorization (RMA).

# 3.6  Replace an Electrical Interface Assembly

You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

**Step 1**    To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly (Figure 3-6).

**Step 2**    Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.

> **Note**  If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

**Step 3**    If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.

**Step 4**    If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.

> **Note**  Attach backplane sheet metal covers whenever EIAs are not installed.

**Step 5**    Line up the connectors on the new EIA with the mating connectors on the backplane.

**Step 6**    Gently push the EIA until both sets of connectors fit together snugly.

**Step 7**    Replace the nine perimeter screws that you removed while removing the backplane cover.

**Step 8**    If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

**Step 9**    Reattach the lower backplane cover.

# 3.7  Replace the Small-Formfactor Pluggable Connector

**Step 1**    Unplug the SFP connector and fiber from the ML-series Ethernet card.

**Step 2**    If the SFP connector has a latch securing the fiber-optic cable, pull it upward to release the cable.

**Step 3**    Pull the fiber cable straight out of the connector.

**Step 4**    Plug the fiber into a Cisco-supported SFP connector.

**Step 5**    If the new SFP connector has a latch, close the latch over the cable to secure it.

**Step 6**    Plug the cabled SFP connector into the ML-series Ethernet card port until it clicks.

**C H A P T E R 4**

# Error Messages Troubleshooting

---

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

---

This chapter explains how to troubleshoot commonly-encountered error messages for the Cisco ONS 15454. The error dialog box consists of two parts: the error title and the error message.

***Figure 4-1    An Error Dialog Box***
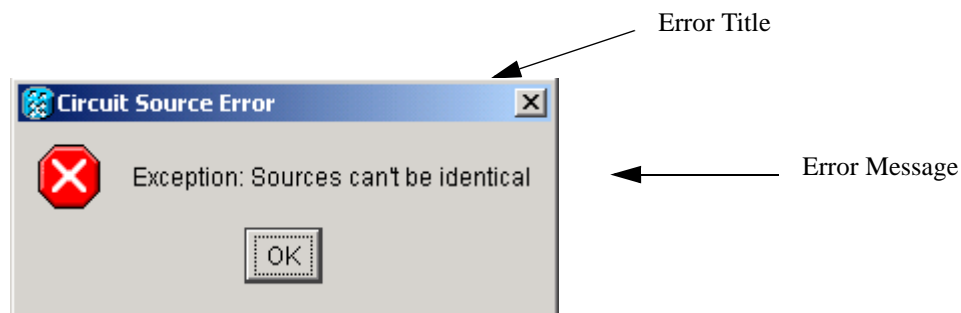


Sections in this chapter are divided into error type (for example, circuit errors, BLSR errors, etc.) followed by the error title(s) for each dialog.

## 4.1  Circuit Errors

This section includes circuit-related error messages. The following headings show the error title (e.g. 4.1.x). If the same error title has multiple error messages, the error messages are listed as subheadings (e.g. 4.1.x.x)

## 4.1.1 Circuit Source Error

The following messages appear in the Circuit Source Error dialog box. For detailed circuit creation instructions, refer to the *Cisco ONS 15454 Procedure Guide*.

### 4.1.1.1 Exception: Source node must be selected

This error message appears if you click Next on the Circuit Source Creation dialog box without entering a source node.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Choose the primary source node for the circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the primary source.

**Step 4**    Click **Next**.

### 4.1.1.2 Exception: Source is not fully specified

This error message appears when the source circuit is not fully defined.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Choose the primary source node for the circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the primary source.

**Step 4**    Click **Next**.

### 4.1.1.3 Exception: Secondary Source is not fully specified

This error message appears when the secondary circuit is not fully defined.

**Step 1**    Click **OK** to close the dialog box.

**Step 2**    Choose the secondary source node for the circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the secondary source.

**Step 4**    Click **Next**.

### 4.1.1.4 Exception: Sources can't be identical

This error occurs if identical primary and secondary source circuits are selected.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Click the **Use Secondary Source** button.

**Step 3**    Choose a Slot, Port and STS or VT number, if applicable, that is not the same as the primary circuit.

**Step 4**    Click **Next**.

# 4.1.2 Circuit Destination Error

The following error messages appear in the Circuit Destination Error dialog box.

## 4.1.2.1 Exception: Destination node must be selected

This error message appears if you do not select a destination node and try to proceed to the next circuit creation screen.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Choose the primary destination node for the circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the primary destination.

**Step 4**    Click **Next**.

## 4.1.2.2 Exception: Destination is not fully specified

This error message occurs when the destination circuit is not fully defined.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Choose the primary destination node for circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the primary source.

**Step 4**    Click **Next**.

## 4.1.2.3 Exception: Secondary Destination is not fully specified

This error message occurs when the secondary destination circuit is not fully defined.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Choose the secondary destination node for the circuit.

**Step 3**    Choose the Slot, Port, STS and VT if applicable for the secondary destination.

**Step 4**    Click **Next**.

## 4.1.2.4 Exception: Destinations can't be identical

This error occurs if primary and secondary circuit destinations are selected.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Click the "Use Secondary Destination" button.

**Step 3**    Choose a Slot, Port and STS or VT number if applicable that is not the same as the primary circuit.

**Step 4**    Click **Next**.

## 4.1.3 Circuit Destroy Failed

The following messages appear in the Circuit Destroy Failed dialog box.

These errors occur when a circuit is being deleted and CTC loses DCC or gateway LAN communication to the node.

### 4.1.3.1 CmsCommFailException: < node-ip address > Communications error (COMM_FAILURE) while attempting to set the CircuitModel.delete attribute

CTC cannot communicate with all the nodes in the network where the circuit must traverse. CTC must be able to communicate with all of the nodes before it is safe to delete the circuits.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Go to the network view and verify that none of the nodes are greyed out

**Step 3**    Click the **Alarms** tab.

**Step 4**    Search for alarms to indicate that there is a DCC termination failure.

**Step 5**    If a DCC termination failure is present, reprovision the DCC channel or check for a broken fiber between the two nodes.

**Step 6**    If a DCC termination failure is not present, access a command prompt from CTC and run the ping command to the nodes the circuit traverses. See the "Ping the ONS 15454" procedure on page 1-53.

**Step 7**    Repeat Step 6 as needed to verify that CTC can successfully run the ping command to each of the nodes.

**Step 8**    Click the **Circuit** tab in either the network view or node view.

**Step 9**    Highlight the circuit that you need to delete.

**Step 10**   Click the **Delete** button.

**Step 11**   Click the **Yes** button when the circuit deletion warning dialog box appears.

**Step 12**   Delete as many circuits as necessary.

### 4.1.3.2 CmsCommFailException: < node-ip address > The Node was not initialized while attempting to set the CircuitModel.delete attribute

CTC cannot communicate with all the nodes in the network where the circuit must traverse. CTC must be able to communicate with all of the nodes before it is safe to delete the circuits.

**Step 1**    Click **OK** to close the error dialog box.

**Step 2**    Go to the network view and verify that none of the nodes are greyed out

**Step 3**    Click the **Alarms** tab.

**Step 4**    Search for an alarms to indicate that there is a DCC termination failure.

**Step 5** If a termination failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes.

**Step 6** If an SDCC termination failure is not present, run the ping command to the nodes the circuit traverses. See the "Ping the ONS 15454" procedure on page 1-53.

**Step 7** Verify that CTC can successfully run the ping command to each of the nodes.

**Step 8** Click the **Circuit** tab in either the network or node view.

**Step 9** Highlight the circuit that you want to delete.

**Step 10** Click the **Delete** button.

**Step 11** Click the **Yes** button when the circuit deletion warning dialog box appears.

**Step 12** Delete as many circuits as necessary.

# 4.1.4  Auto-Ranging Circuit Creation

The following messages appear in the Auto-Ranging Circuit Creation dialog box.

### 4.1.4.1  Unable to provision circuit Unexpected exception encountered Attempts to access a VtAdit that has been destroyed.CmsObjectNotExistException: Attempts to access a VtAdit that has been destroyed.

This error occurs when routing a group of VT circuits over an existing VT tunnel.

This error typically occurs when a CTC session attempts to access a VT-grooming STS Path that has been deleted by another CTC user (or session).

**Step 1** Click **OK** to clear the error dialog box.

**Step 2** Cancel the circuit dialog box.

**Step 3** Restart the circuit dialog box.

**Step 4** Continue to provision the original circuit.

### 4.1.4.2  NoRoute: ComputerRouteInMixedDomains: No Route found with given  requirements.

This error occurs when CTC attempts to create autoranged circuits but it cannot provision a route for the subsequent circuits. One of the protection paths is fully blocked because there is no available bandwidth after the Nth circuit is attempted.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.

- One or more VT Tunnels were required to complete a VT circuit but a failure was encountered during the provisioning of the tunnels.

- A BLSR was along the path but there was no common time slot available in the ring.

- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:

  - A node along the path from source to drop was "excluded" and no other path is available.

  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).

  - One of the required links does not have bandwidth to support the circuit.

  - One of the required links for a path-protected circuit cannot be protected

If a circuit routing failure is encountered, identify the root cause of the problem among the above set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

---

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Calculate how much available bandwidth is available on both the working and the protection path by following the steps below.

    **a.**    Go to the network view on the CTC.

    **b.**    Click on each span and then right-click the mouse button.

    **c.**    Click the **Circuits** label from the drop down screen. A table appears that shows the available bandwidth.

    **d.**    Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working and a protection path.

**Step 3**    Click **Create** on the main circuit screen.

**Step 4**    Input the number of available circuits based on the available bandwidth into the **Number of Circuits** box.

**Step 5**    Click **Next** at the bottom of the screen.

**Step 6**    Continue to provision both the source and destination circuits.

**Step 7**    Click **Finish** on the Circuit Routing Preferences screen.

---

### 4.1.4.3  Unable to drop route ComputeRouteInMixedDomains: No Route found with given requirements NoRoute: ComputeRouteInMixedDomains: No Route found with given requirements

This error is very similar to the previous error, but applies to drop circuits only. Both of the errors can occur when a path is no longer available.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.

- The network topology has not been fully discovered.

- Sufficient network bandwidth is not available to support the requested circuit.

- Path protection was requested and there is no end-to-end protected path available.

- A BLSR was along the path but there was no common time slot available in the ring.

- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:

  – A node along the path from source to drop was "excluded" and no other path is available.

  – A required link along the path from source to drop was selected in the wrong direction (from drop to source).

  – One of the required links does not have bandwidth to support the circuit.

  – One of the required links for a path-protected circuit cannot be protected

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Calculate how much available bandwidth is available on both the working and the protection path by following the steps below.

a.    Go to the network view on the CTC.

b.    Click on each span and then right-click the mouse button.

c.    Click the **Circuits** label from the drop down screen. A table appears that shows the available bandwidth.

d.    Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working and a protection path.

**Step 3**    Click **Create** on the main circuit screen.

**Step 4**    Input the number of available circuits based on the available bandwidth into the **Number of Circuits** box.

**Step 5**    Click **Next** at the bottom of the screen.

**Step 6**    Continue to provision both the source and destination circuits.

**Step 7**    Click **Finish** on the Circuit Routing Preferences screen.

## 4.1.4.4  NoRoute: Unable to route VT Circuit: possible reasons: 1) VT Tunnel required and cannot route due to XCs in the path from source to destination 2) Cannot find route that satisfies given requirements

This exception occurs if a one or more lower order VT tunnels were required to complete a VT circuit but a failure was encountered during the provisioning of the tunnels.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Provision the VT circuit.

## 4.1.4.5  Exception: Source is not fully specified

This error occurs when more auto-ranged circuits are requested than the available ports or STSs can accomodate. For example, if a user attempts to automatically provision 15 DS3 circuits and there is only one 12-port DS3 card in the system, the error will appear after all 12 DS3 ports are utilized. The auto-ranging circuit provisioning does not automatically increment the slot for the source or destination. It does not automatically increment the port number on the OC-3 card for STS-1 circuits.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Click **Back**.

Step 3    Provision more ports on the system to satisfy the available auto-ranging requirements.

Step 4    Insert additional cards if slots are available.

Step 5    The installed card should reflect the type of circuit that is being added (i.e. DS-3, DS-1, etc.)

Step 6    If more slots are unavailable, the number of auto ranged circuits must be reduced.


## 4.1.5 Node Selection Error

The following message appears in the Node Selection Error dialog box.

### 4.1.5.1 Failure getting list of available ports from <node-name> <node ipaddress> Communications error (COMM_FAILURE) while attempting to get the ConnectionModels.availEntitiesForVtsPath attribute.

This specific error occurred when DCC was taken down during the auto creation of VT circuits.

The general cause of the problem is loss of connectivity to one of the nodes in the network. A deleted DCC is one of the specific reasons for loss of connectivity. Another reason might be IP routing failures due to static route reconfiguration.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Go to the network view and verify that none of the nodes are greyed out.

Step 3    Click the **Alarms** tab and search for alarms to indicate an SDCC failure.

Step 4    If an SDCC failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes, then continue provisioning the circuit.

Step 5    If an SDCC failure is not present, run the ping command to the nodes the circuit traverses. See the "Ping the ONS 15454" procedure on page 1-53.

Step 6    Verify that CTC can successfully run the ping command to each of the nodes.

Step 7    Click the **Circuit** tab in either the network or node view.

Step 8    Click the **Create** button.

Step 9    Continue provisioning the circuit.

✎
Note    During the auto creation process verify that the network is stable by watching for the greying out of nodes or SDCC alarm messages.

# 4.1.6 Circuit Creation Error

The following messages appear in the Circuit Creation Error dialog box.

## 4.1.6.1 Circuit creation cannot proceed due to changes in the network, which affect the circuit(s) being created. The dialog box will close. Please try again.

This error message occurs if a network change occurs simultaneously to circuit provisioning.

**Step 1**   Click **OK** to clear the error dialog box.

**Step 2**   Go to the network view and verify that none of the nodes are greyed out

**Step 3**   Click the **Alarms** tab and search for alarms that indicate an SDCC failure.

**Step 4**   If an SDCC failure is present, reprovision the SDCC channel or check for a broken fiber between the two nodes, then continue provisioning the circuit.

**Step 5**   If an SDCC failure is not present, run the ping command to the nodes the circuit traverses. See the .

**Step 6**   Verify that CTC can successfully run the ping command to each of the nodes.

**Step 7**   Click the **Circuit** tab in either the network or node view.

**Step 8**   Click the **Create** button.

**Step 9**   Continue provisioning the circuit.

# 4.1.7 Error While finishing Circuit Creation

The following messages appear in the Error While Finishing Circuit Creation dialog box.

## 4.1.7.1 Unable to provision circuit No VT-capable STSs are available at <node-name>

The maximum number of cross- connections that can be created on the ONS 15454 has been reached. The user can not proceed any further until some circuits are deleted.

Each VT1.5 cross-connection takes up one slot in two or more VT-grooming STSs on the node.

Only 24 VT-grooming STSs are available at each node. Hence, the maximum number of VT1.5 cross-connections possible on a given node depends on the type of connections and the configuration. For example, if all cross-connections were simple 2-way type connections and all 24 STSs were fully packed, the maximum number is 336 (= 24*28/2).

**Step 1**   Click **OK** to clear the error dialog box.

**Step 2**   Go to the node view and click the **Circuit** tab.

**Step 3**   Highlight some circuits that need to be deleted.

**Step 4**   Click the **Delete** button.

**Step 5**   Click on **Yes** when the warning dialog box appears.

**Step 6**   Create another circuit to replace the deleted circuit.

**Note** There is a finite number of cross-connections that can be provisioned on the ONS 15454. To add more cross-connections, existing cross-connections must be deleted.

## 4.1.7.2  Unable to provision circuit Circuit provision error Unable to create connection at <node-name>

This error occurs when two users attempt to provision the same circuit simultaneously. The error message also occurs when connectivity is lost to the node being provisioned during circuit creation.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Delete the created circuit.

**Step 3**    Coordinate with the other user when provisioning circuit across the same equipment.

## 4.1.7.3  NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements.

This error occurs when CTC cannot provision a route for auto-ranged circuits.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Free up some available bandwidth on the blocked path or route the circuit along an unprotected path with some available bandwidth. To determine the available bandwidth:

    **a.**    Go to the network view.

    **b.**    Click each span and then right-click the mouse button.

    **c.**    Click the **Circuits** label from the drop down screen. A table will appear that shows the available bandwidth.

    **d.**    Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.

**Step 3**    Click **Create** on the main circuit screen.

**Step 4**    Input the circuit attributes - Name, Type, Size.

**Step 5**    Click **Next**.

**Step 6**    Continue to provision both the source and destination circuits.

## 4.1.7.4  Circuit sanity check failed. Invalid connection at node <node name> SanityCheckFailed: Invalid connection at node <node name>.

The error message appears if a path protection configuration connection cannot be created due to a protected source or destination endpoint.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Click **Back**.

Step 3    Unclick **Use Secondary Destination**.

Step 4    Click **Back**.

Step 5    Unclick **Use Secondary Source**.

Step 6    Click **Next**.

Step 7    Choose the same node for the destination circuit as is chosen for the source circuit.

Step 8    Choose destination slot, port, STS and VT parameters for both the primary and secondary circuits.

Step 9    Click **Finish**.

## 4.1.7.5    CmsObjectNotExistException: Attmpt to access the CtAditModel.getAvailableSts attribute for an object that does not exist.

This error occurs when a user attempts to access a VT-grooming STS Path that has been deleted by another user. Reattempt the circuit provisioning after canceling out the circuit dialog box.

## 4.1.7.6    Circuit spans verification: selected spans are invalid! Invalid span combination at Node <node name> SanityCheckFailed: Invalid span combination at Node <node name>

This error message is related to the validity of the input and output paths at each circuit node that result from the selection of spans during manual routing.

**Note**    Circuit sources and drops are also considered paths, but it is the selection of spans that occurs during manual routing. The sources and drops are fixed during this phase of circuit creation.

Like the "Invalid connection at node <node name>" error message, it identifies invalid situations where a selector path of a path protection configuration selection has line-level protection. The selector paths are circuit spans rather than source or destination endpoints.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Choose additional spans from source node to the destination node.

Step 3    Choose a second span if the circuit is to be path protected from source node to destination node.

Step 4    Click **Finish**.

## 4.1.7.7    Circuit spans verification″ selected spans are invalid! Link Diverse Path requirement is not met. The link is <node name source -> <node name destination> (LINK_VTT unprot, State=Up). Node Check is the link is a VT Tunnel

This error occurs if link diversity is requested for a VT circuit and the tunnels selected do not traverse different paths.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Go to the "Route Review and Edit" screen.

Step 3    Select one of the spans that traverses a tunnel.

Step 4    Click **Remove**.

The span should disappear on the screen.

Step 5    Click a span that does not follow the original tunnels path.

Step 6    Continue to route the circuit path to the destination node by selecting and adding all the necessary spans in the path.

Step 7    Click **Finish**.

## 4.1.7.8  Circuit sanity check failed. Path specified is not protected. Check span <node name> -> <nodename> (LINK_PHYSICAL unprot, State=Up). OCN IsmState=2,2.

This error message appears when a protection path is not provisioned for a manually-routed circuit.

**Note**    An alternative solution is to create line protection (1+1) from source to destination; in this case, a protection path would be inherently included in the circuit route.

Step 1    Click **OK** to clear the error dialog box.

Step 2    Choose a second span from source node to destination node.

Step 3    Click **Finish**.

## 4.1.7.9  Circuit sanity check failed. Source/Drop is an endpoint of a network link.

This error message occurs when the user attempts to create a circuit from one trunk side to another trunk side and does not use a dropped circuit.

This error occurs if the source or destination is a trunk endpoint.

Step 1    Go to the Circuit Creation screen.

Step 2    Choose circuit name, type and size.

Step 3    On the circuit source screen provision an STS from the trunk card (e.g the OC-48 supporting the ring).

Step 4    On the circuit destination screen provision an STS from the trunk card.

Step 5    Click **Finish**.

Step 6    Click **OK** to clear the error dialog box.

Step 7    Go back and choose only drop side circuits.

## 4.1.7.10  Unable to route drop. ComputerRouteInMixedDomains: No Route found with given requirements. NoRoute: ComputerRouteInMixedDomains: No Route found with given requirements

This error occurs when no available route around the ring is available. For example, one of the required links for a path-protected circuit cannot be protected. If a circuit routing failure is encountered, identify the root cause of the problem among the following set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.
- One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
- A BLSR was along the path but there was no common time slot available in the ring.
- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
  - A node along the path from source to drop was "excluded" and no other path is available.
  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
  - One of the required links does not have bandwidth to support the circuit.

**Step 1**   Click **OK** to clear the error dialog box.

**Step 2**   Go to the network view.

**Step 3**   Click each span and then right-click the mouse button.

**Step 4**   Click the **Circuits** label from the drop down screen.

A table will appear which shows the available bandwidth.

**Step 5**   Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.

**Step 6**   Click **Create** on the main circuit screen.

**Step 7**   Provision the circuit attributes (Name, Type, Size).

**Step 8**   Click **Next**.

**Step 9**   Continue to provision both the source and destination circuits.

# 4.1.8  Error Adding Drop

The following messages appear in the Error Adding Drop dialog box.

### 4.1.8.1 SanityCheckFailed: Source/Drop is an endpoint of a network link

This error occurs during one-way circuit provisioning when an additional drop to a trunk or network port is attempted.

**Step 1**  Go to the Circuit Creation screen.

**Step 2**  Choose the circuit name, type, and size.

**Step 3**  Uncheck the **Bidirectional** circuit box.

**Step 4**  Choose an unprotected source and destination circuit between two spans.

**Step 5**  Go back and highlight the original circuit.

**Step 6**  Click **Edit**.

**Step 7**  Click the **Drop > Create** tabs.

**Step 8**  Add a circuit on the trunk of network side.

**Step 9**  Click **OK** to clear the error dialog box.

**Step 10**  Choose a circuit that is on the drop side (not on the trunk side).

### 4.1.8.2 Exception: Drop node must be selected

This error occurs when the drop node is not selected.

**Step 1**  Click **OK** to clear the error dialog box.

**Step 2**  Choose a node to drop the circuit.

**Step 3**  Choose slot, port, STS, and VT if applicable.

**Step 4**  Click **OK**.

### 4.1.8.3 Circuit provisioning error Unable to add output to connection at <node-name> Path already in use

This error occurs when two CTC sessions are simultaneously provisioning circuits using the same path.

**Step 1**  Click **OK** to clear the error dialog box.

**Step 2**  Coordinate with the operator attempting to provision a circuit on the same path.

**Step 3**  Recreate the circuit.

## 4.1.9 Error Applying Changes

The following message appears in the Error Applying Changes dialog box.

### 4.1.9.1  InvalidProtectionOp: Unable to switch. A higher priority request may be present.

This error occurs when a user attempts to activate a path protection configuration switch and another user has already made a higher priority request.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Choose **Clear**.

**Step 3**    Click **Apply**.

**Step 4**    Choose new switch command.

**Step 5**    Click **Apply**.

## 4.1.10  Error Deleting Circuit Drop

The following messages appear in the Error Deleting Circuit Drop dialog box.

### 4.1.10.1  IncorrectCircuitState: Circuit drop can be deleted only when state is CREATING, ACTIVE or DROP_PENDING

This error occurs if the user attempts to delete dropped circuits that are not in the correct state.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Click the **Delete** button again after circuits are in the proper state.

### 4.1.10.2  CannotDeleteLastDrop: Last circuit drop cannot be deleted. Please destroy the circuit instead

This error occurs when deleting a group of dropped circuits and one circuit is left which represents the original circuit. The circuit must be deleted from the main circuit screen.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Go to the main circuit screen and delete the circuit.

**Note**    The user can not delete the entire circuit from the drop screen. To delete the entire circuit, the user must go to the main circuit provisioning screen and then delete the circuit.

# 4.1.11 Error

The following circuit-related messages appear in the Error dialog box. (See also the "Error" section on page 4-23 for BLSR-related messages that appear in this dialog box.)

### 4.1.11.1 Please select a node first

This error occurs when the user attempts to select a path while manually routing a circuit and a source node is not selected.

**Step 1** Click **OK** to clear the error dialog box.

**Step 2** Click on source node.

**Step 3** Select only paths with a green arrow.

**Step 4** Continue routing the circuit.

### 4.1.11.2 This link may not be included in the required list. Constraints only apply to the primary path.

This error occurs during automatic circuit provisioning when the user checks Using Required Nodes/Spans and Nodal Diversity and the Required list contains only one route. The second protection route is automatically created.

**Step 1** Click **OK** to clear the error dialog box.

**Step 2** Choose only one primary path.

**Step 3** Click **Finish**.

### 4.1.11.3 This node is not selectable: Only the Source node and nodes attached to included (blue) are selectable. Selecting a selectable node will enable its available outgoing spans

This error occurs when the a non-source node is selected in the manual routing area.

**Note** Apart from the source node, it is also valid to select nodes attached to the spans that are already selected for this circuit. This error will appear if you select any other node.

**Step 1** Click **OK** to clear the error dialog box.

**Step 2** Click the source node.

**Step 3** Click an available span designated by a green arrow.

**Step 4** Click **Add Span**.

**Step 5** Click the next span in sequence towards the green arrow.

**Step 6** Click **Add Span**.

**Step 7** If this is a protected span, complete a second protection path.

**Step 8**    Click **Finish**.

### 4.1.11.4  This span is not selectable. Only green spans with arrows.

This error appears when selecting a manual route that has a green line and not a green arrow.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Go back and choose only green arrows.

### 4.1.11.5  Sorry, no paths are available on this link.  Please make another selection.

This error occurs when a user selects an unavailable path for a manually-routed circuit.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Reroute the circuit around a path with available bandwidth.

**Step 3**    Click **Finish**.

### 4.1.11.6   This link may not be included in the required list. Only 1 outgoing link may be included for each node.

This error occurs when the user checks Using Required Nodes/Spans while provisioning an automatically-routed circuit. The circuit is set up to be unprotected. The required list can contain only one route.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Do not click on more than one link from the source.

**Step 3**    Complete the circuit to the destination by selecting the remaining link.

## 4.1.12  Circuit Deletion Error

The following message appears in the Circuit Deletion Error dialog box.

### 4.1.12.1  DeletionError: Following Circuits Could Not Be Scheduled for Deletion . Error deleting circuit TUN_<node name> ::10:cerent.cms.ncp. SanityCheckFailed: VT Tunnel is in use.

The error occurs when the user tries to delete a VT tunnel before deleting the VT circuit.

> **Note** More than one VT circuit may be using the same VT tunnel; all circuits must be deleted before the tunnel can be deleted.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Highlight the VT circuit in the VT tunnel on the circuit screen.

**Step 3**    Click the **Delete** button.

**Step 4**    Highlight the VT tunnel on the circuit screen.

**Step 5**    Click the **Delete** button.

## 4.1.13 Circuit Attributes Error

The following messages appear in the Circuit Attributes Error dialog box.

### 4.1.13.1 Exception: Circuit name is too long(max 48))

This error occurs when a circuit name is assigned more than 48 characters.

> **Note** For auto-ranged circuits, the maximum circuit-name length is 43 characters.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter a circuit name that is less than or equal to 48 characters.

**Step 3**    Click **Next**.

### 4.1.13.2 NumberFormatException

This error occurs after clearing the Inter-domain Service Level value and proceeding to the next screen.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter the Inter-domain Service Level value using a positive integer.

**Step 3**    Click **Next**.

### 4.1.13.3 NumberFormatException:99999999999999

This error occurs if the Inter-domain Service Level value is too large.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter the proper Inter-domain Service Level value.

**Step 3**    Click **Next**.

### 4.1.13.4  Exception: Number of Circuit must be a positive integer

This error occurs if the Number of Circuits value is too large, is not an integer, or is left blank.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Clear the Number of Circuits box.

**Step 3**    Enter a smaller circuit ranging number.

## 4.1.14  Error Validating Slot Number

The following message appears in the Error Validating Slot Number dialog box.

### 4.1.14.1  Please enter a valid value for the Slot Number

This error occurs if a bad slot number is applied to the circuit filter tool.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter a valid slot number.

**Step 3**    Click **OK**.

## 4.1.15  Error Validating Port Number

The following message appears in the Error Validating Port Number dialog box.

### 4.1.15.1  Please enter a valid value for the Port Number

This error occurs if a bad port number is applied to the circuit filter tool.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter a valid port number.

**Step 3**    Click **OK**.

## 4.1.16  Circuit Route Constraints Error

The following message appears in the Circuit Route Constraints Error dialog box.

### 4.1.16.1  Unable to route drop Compute. RouteInMixedDomains: No Route found with given requirements. NoRoute: ComputeRouteInMixedDomains: No Route found with given requirements.

This error occurs when circuit routing fails; a path is no longer available. This error applies to drop circuits only.

If a circuit routing failure is encountered, identify the root cause of the problem among the following set of conditions. If possible, rectify the problem and re-attempt circuit provisioning.

Circuit routing can fail for one of the following reasons:

- There is no connectivity between the source and drop of the circuit.
- The network topology has not been fully discovered.
- Sufficient network bandwidth is not available to support the requested circuit.
- Path protection was requested and there is no end-to-end protected path available.
- One or more LO Tunnels were required to complete a LO circuit but a failure was encountered during the provisioning of the tunnels.
- A BLSR was along the path but there was no common time slot available in the ring.
- The "Route using Required Nodes/Spans" option was selected and an invalid set of constraints was provided. Examples of invalid constraints include:
  - A node along the path from source to drop was "excluded" and no other path is available.
  - A required link along the path from source to drop was selected in the wrong direction (from drop to source).
  - One of the required links does not have bandwidth to support the circuit.

**Step 1**  Click **OK** to clear the error dialog box.

**Step 2**  Go to the network view.

**Step 3**  Click each span and then right-click the mouse button.

**Step 4**  Click the **Circuits** label from the drop down screen.

A table will appear which shows the available bandwidth.

**Step 5**  Make a note of the available bandwidth for each of the spans. Note the available bandwidth for both a working a protection path.

**Step 6**  Click **Create** on the main circuit screen.

**Step 7**  Provision the circuit attributes (Name, Type, Size).

**Step 8**  Click **Next**.

**Step 9**  Continue to provision both the source and destination circuits.

# 4.2 BLSR Errors

This section includes BLSR-related error messages. The following headings (4.2.x) show the error title. If the same error title has multiple error dialog boxes, the error dialog boxes are listed as subheadings.

## 4.2.1 Cannot Delete Ring

The following message appears in the Cannot Delete Ring dialog box.

### 4.2.1.1  There is a protection operation set. All protection operations must be clear for ring to be deleted.

This error occurs while a BLSR switch is active and the user attempts to delete the ring.

| | |
|---|---|
| **Step 1** | Click **OK** to clear the error dialog box. |
| **Step 2** | Click the **Conditions** tab. |
| **Step 3** | Double-click the target ring (the ring you will delete) to display the BLSR Edit Window. |
| **Step 4** | The following protection switches are possible: Lockout Span, Force Ring, Force Span, Manual Ring, Manual Span, Exercise Ring, and Exercise Span. These can be identified by the letters L, F, M, and E inside the port. Find a port on the edit map with one of these letters present. |
| **Step 5** | Right-click the port and select **set East/West protection op**. |
| **Step 6** | Select **Clear** and click **OK**. |
| **Step 7** | Click **Yes** on the "Confirm BLSR Operation" dialog box. |
| **Step 8** | Return to the BLSR Provisioning tab in the network view. |
| **Step 9** | Reattempt to delete the ring. |

## 4.2.2 Invalid Ring ID

The following message appears in the Invalid Ring ID dialog box.

### 4.2.2.1 RingID must be an integer between 0 and 9999

This error occurs if a Ring ID greater than 9999 is selected in the BLSR configuration wizard. This error can also occur if a negative number or sequence of alpha characters is entered.

| | |
|---|---|
| **Step 1** | Click **OK** to clear the error dialog box. |
| **Step 2** | Enter a Ring ID between 0 and 9999. |
| **Step 3** | Click **Next**. |

# 4.2.3 Error

The following messages appear in the Error dialog box.

## 4.2.3.1 The Ring ID value is not valid . Please enter a valid number between 0 and 9999.

This error occurs if a BLSR Ring ID is changed to a number greater than 9999 or a string of alpha characters.

**Step 1**     Click **OK** to clear the error dialog box.

**Step 2**     Enter a Ring ID between 0 and 9999

**Step 3**     Click **Apply**.

**Step 4**     Click **OK** when the "Are you sure?" dialog box appears.

## 4.2.3.2 Cannot set reversion to INCONSISTENT!

This error occurs if INCONSISTENT is selected in the BLSR wizard.

**Step 1**     Click **OK** to clear the error dialog box.

**Step 2**     Choose a reversion time between .5 and 12 minutes, or choose "never."

**Step 3**     Click **Apply**.

## 4.2.3.3 You must enter a number and it must be between 0 and 31.

This error occurs in the BLSR wizard edit screen when the node ID entered is not between 0 and 31.

**Step 1**     Click **OK** to clear the error dialog box.

**Step 2**     Click **Cancel** to close the Edit ID window.

**Step 3**     Examine the BLSR wizard edit window to determine the node IDs in the ring. The node ID is the number in parentheses next to the node name in the edit map.

**Step 4**     Right-click the node whose ID you wish to change and select **Set Node ID**.

**Step 5**     Enter a node ID between 0-31 that is not already in use.

**Step 6**     Click **OK**.

## 4.2.3.4 Error - this node ID is already in use. Please choose another.

This error occurs if the user chooses a duplicate node ID.

**Step 1**     Click **OK** to clear the error dialog box.

**Step 2**    Click **Cancel** to close the Edit ID window.

**Step 3**    By examining the BLSR wizard edit window determine the node IDs in the ring. The node ID is the number in parentheses next to the node name in the edit map.

**Step 4**    Right-click the node with the node ID you need to change and select **Set Node ID**.

**Step 5**    Enter a node ID between 0-31 that is not already in use.

**Step 6**    Click **OK**.

# 4.2.4  Error Applying Changes

The following messages appear in the Error Applying Changes dialog box.

### 4.2.4.1  Exception: Unable to switch East Line, a higher priority request may be present.

This error occurs when an existing request is present and a lower order request is attempted.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Go to the East Switch BLSR box and choose a switch of equal or higher priority than the switch in the West Switch BLSR box.

**Step 3**    Go to the network view.

**Step 4**    Click the **Provisioning** > **BLSR** tabs.

**Step 5**    In the edit map double-click on the BLSR.

**Step 6**    Identify the port in the ring with a protection operation. The port will have an L, F, M, or E present.

**Step 7**    Right-click the port, clear the protection operation, and click **OK**.

**Step 8**    Right-click the desired port, change the protection operation, and click **OK**.

### 4.2.4.2  Exception: Unable to switch West Line, a higher priority request may be present.

This error occurs when an existing request is present and a lower order request is attempted.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Go to the West Switch BLSR box and choose a switch of equal or higher priority than the switch in the East Switch BLSR box.

**Step 3**    Go to the network view.

**Step 4**    Click the **Provisioning** > **BLSR** tabs.

**Step 5**    In the edit map double-click on the BLSR.

**Step 6**    Identify the port in the ring with a protection operation. The port will have an L, F, M, or E present.

**Step 7**    Right-click the port, clear the protection operation, and click **OK**.

**Step 8**    Right-click the desired port, change the protection operation, and click **OK**.

# 4.2.5  Duplicate Node ID

The following message appears in the Duplicate Node ID dialog box.

## 4.2.5.1  New Node ID (N) for Ring ID N duplicate ID of node <ip address>

This error occurs when an existing node ID is selected from the BLSR provisioning screen.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Go to one of the nodes in the ring.

**Step 3**    Click the **Provisioning > BLSR** tabs.

**Step 4**    Click the **Ring Map** button.

**Step 5**    Observe the node ID numbers in the ring map table.

**Step 6**    Choose a node ID number between 0 and 31 that is not already in use.

**Step 7**    Click **Apply**.

# 4.2.6  BLSR Error

The following messages appear in the BLSR Error dialog box.

## 4.2.6.1  Exception: West and East ports must be different

This error occurs if a BLSR is provisioned to use the same slot for both the east and west lines.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Make sure the West Line and the East line are not using the same slot.

**Step 3**    Click **OK**.

## 4.2.6.2  Exception: West and East ports must have the same line rate

This error occurs if a BLSR is provisioned using different line rates for the east and west lines.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Make sure the West Line and the East line are not using different line rates.

**Step 3**    Click **OK**.

## 4.2.6.3 Exception: Unable to parse Ring ID

This error occurs if a bad value is chosen when provisioning a BLSR span, such as an alpha character, a number that is too large, or no number at all.

**Step 1**    Click **OK** to clear the error dialog box.

**Step 2**    Enter a ring ID between 0 and 9999

**Step 3**    Click **OK**.

## M

# X