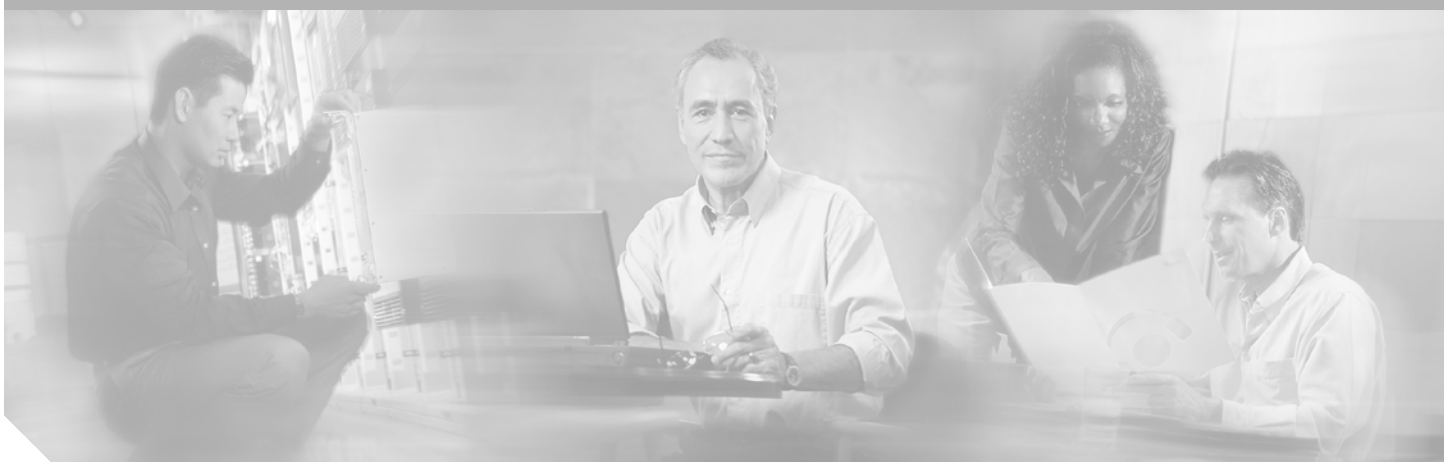
CISCO SYSTEMS



Cisco ONS 15454 Procedure Guide

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

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

Customer Order Number: DOC-7815934=
Text Part Number: 78-15934-02

CONTENTS

FIGURES

TABLES

PROCEDURES

TASKS

About this Guide

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

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

Revision History

Date	Notes
03/30/2007	Revision History Table added for the first time
08/20/2007	Updated About this Guide

This section provides the following information:

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

Document Objectives

This guide provides procedures for installation, turn up, provisioning, and acceptance of ONS 15454 nodes and ONS 15454 networks.

Audience

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

Document Organization

The organization of the guide reflects Cisco's recommended work flow for new installations. This organization also provides easy access to procedures and tasks used to modify existing installations. Verification procedures are provided, where necessary, to allow contract vendors to complete the physical installation and then turn over the site to craft personnel for verification, provisioning, turn up, and acceptance.

The front matter of the book appears in the following sequence:

1. Title Page
2. Table of Contents
3. List of Figures
4. List of Tables
5. List of Procedures
6. List of Tasks

The information in the book follows a task-oriented hierarchy using the elements described below.

Chapter (Director Level)

The guide is divided into logical work groups (chapters) that serve as director entry into the procedures. For example, if you are arriving on site after a contractor has installed the shelf hardware, proceed to Chapter 2, "Install Cards and Fiber-Optic Cable" and begin verifying installation and installing cards. You may proceed sequentially (recommended), or locate the work you want to perform from the list of procedures on the first page of every chapter (or turn to the front matter or index). Table 1 describes the guide chapters.

Table 1 Cisco ONS 15454 Procedure Guide Chapters

Title	Summary
Chapter 1, "Install the Shelf and Backplane Cable"	Includes procedures for installing the shelf assembly, electrical interface assemblies (EIAs), power and ground, fan-tray assembly, alarm expansion panel, backplane wires, external wire-wrap panel, electrical card cables, and optional dense wavelength division multiplexing (DWDM) equipment. Also included is the shelf installation acceptance test.
Chapter 2, "Install Cards and Fiber-Optic Cable"	Includes procedures to install common control cards, optical cards, transponder and muxponder cards, electrical cards, Ethernet cards and connectors, FC_MR-4 cards, and DWDM cards. Also included are procedures for removing and replacing a card, preprovisioning a slot, and installing and routing fiber-optic cables.
Chapter 3, "Connect the PC and Log into the GUI"	Includes procedures to install the Cisco Transport Controller (CTC), set up a computer for different connection types, and log into the Cisco ONS 15454.
Chapter 4, "Turn Up Node"	Includes procedures to verify the card installation; create users and assign security; set up name, date, time and contact information; set up network access, firewall access, and timing; create protection groups; and provision Simple Network Management Protocol (SNMP).
Chapter 5, "Turn Up a DWDM Node"	Includes procedures to verify TCC2 card installation and provision the DWDM node.
Chapter 6, "Turn Up Network"	Includes procedures to verify the node turn up, and provision and test the following networks: point-to-point, linear ADM, bidirectional line switched ring (BLSR), and path protection. It also includes procedures for subtending rings.
Chapter 7, "Turn Up DWDM Network"	Includes procedures to verify DWDM node turn up; provision DWDM or hybrid network connections; run automatic node setup; verify optical service channel module power; and perform a hub or terminal node acceptance test.
Chapter 8, "Create Circuits and VT Tunnels"	Includes procedures to verify network turn up; create manually or automatically routed circuits or VT tunnels; create unidirectional circuits with multiple drops; create VT aggregation points, half circuits, Ethernet circuits, and overhead circuits; provision a DWDM optical channel network connection; and create virtual concatenated (VCAT) circuits.

Table 1 Cisco ONS 15454 Procedure Guide Chapters (continued)

Title	Summary
Chapter 9, "Manage Alarms"	Includes procedures to document existing node data, view and delete alarms, view alarm-affected circuits and LCD alarm counts, manage alarm profiles, filter alarms, suppress alarms, and provision external alarms.
Chapter 10, "Monitor Performance"	Includes procedures to change the performance monitoring (PM) display, monitor performance, and manage remote monitoring (RMON) thresholds.
Chapter 11, "Manage Circuits"	Includes procedures to view circuits and cross-connect resource usage, modify and delete circuits and tunnels, convert and upgrade CTC and TL1 circuits, monitor circuits, and create a J1 path trace.
Chapter 12, "Change Node Settings"	Includes procedures to change node management information, CTC network access and view, and DWDM node settings; change or delete card protection settings; delete SONET data communication channel (DCC), line data communication channel (LDCC), generic communication channel (GCC), and DWDM optical service channel (OSC) terminations; and change node timing, security, and Simple Network Management Protocol (SNMP).
Chapter 13, "Change Card Settings"	Includes procedures to modify line settings and PM parameter thresholds for cards, modify alarm interface controller settings, and upgrade DS-1 and DS-3 1:1 protection to 1:N protection.
Chapter 14, "Upgrade Cards and Spans"	Includes procedures to prevent an OC-N protection switch during cross-connect upgrades, upgrade or downgrade cards, and upgrade spans automatically or manually.
Chapter 15, "Convert Network Configurations"	Includes procedures to convert network configurations, modify a BLSR, and manage BLSR switches.
Chapter 16, "Add and Remove Nodes"	Includes procedures to add or remove BLSR, path protection, or linear nodes from a network configuration.
Chapter 17, "Maintain the Node"	Includes procedures to inspect and manage the air filter, backup and restore the database, restore the node to factory configuration, off load the security audit trail log, inhibit card protection switching, revert software, clean fiber connectors, reset the TCC2 card using CTC, view Ethernet card maintenance information, change the node timing reference, and view the timing report.

Table 1 Cisco ONS 15454 Procedure Guide Chapters (continued)

Title	Summary
Chapter 18, "Power Down the Node"	Includes the procedure to power down the node.
Appendix A, "CTC Information and Shortcuts"	Includes a description of the CTC views and window features.
Appendix B, "Specifications"	Lists the ONS 15454 specifications.

Non-Trouble Procedure (NTP)

Each NTP is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

Note Throughout this guide, NTPs are referred to as "procedures" and DLPs are termed "tasks." Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

Detailed Level Procedure (DLP)

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When the proper response is not obtained, the DLP provides a trouble clearing reference.

Related Documentation

Use the *Cisco ONS 15454 Procedure Guide, R4.6* with the following referenced publications:

- *Cisco ONS 15454 Reference Manual, R4.6*—Provides reference material for the Cisco ONS 15454 node and network.
- *Cisco ONS 15454 Troubleshooting Guide, R4.6*—Provides general troubleshooting procedures, alarm descriptions and troubleshooting procedures, and hardware replacement instructions.
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, R4.6*—Provides a comprehensive list of TL1 commands for the ONS 15454 and ONS 15327.
- *Release Notes for the Cisco ONS 15454, R4.6*—Provides caveats, closed issues, and new feature and functionality information.

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

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

Where to Find Safety and Warning Information

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

Install the Shelf and Backplane Cable

This chapter provides procedures for installing the Cisco ONS 15454. For a summary of the tools and equipment required for installation, see the "Required Tools and Equipment" section on page 1-2.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4—Complete this procedure before continuing with the "NTP-A2 Install the Shelf Assembly" procedure on page 1-6.
2. NTP-A2 Install the Shelf Assembly, page 1-6—Complete this procedure to install the shelf assembly in a rack.
3. NTP-A3 Open and Remove the Front Door, page 1-13—Complete this procedure to access the equipment before continuing with other procedures.
4. NTP-A4 Remove the Backplane Covers, page 1-16—Complete this procedure to access the backplane before continuing with other procedures.
5. NTP-A5 Install the EIAs, page 1-17—Complete this procedure if you plan to install electrical cards. This procedure is a prerequisite to the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-49.
6. NTP-A6 Install the Power and Ground, page 1-25—Complete this procedure before continuing with the "NTP-A7 Install the Fan-Tray Assembly" procedure on page 1-31.
7. NTP-A7 Install the Fan-Tray Assembly, page 1-31—Complete this procedure to install the fan-tray assembly in the shelf.
8. NTP-A119 Install the Alarm Expansion Panel, page 1-34—Complete this procedure if you are planning to install the Alarm Interface Controller–International (AIC-I) card and want to increase the number of alarm contacts provided by the AIC-I card.
9. NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-37—Complete this procedure as needed to set up wire-wrap pin connections.
10. NTP-A120 Install an External Wire-Wrap Panel to the AEP, page 1-44—Complete this procedure to connect an external wire-wrap panel to the alarm expansion panel (AEP).
11. NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-49—Complete this procedure if you plan to install electrical cards.
12. NTP-A10 Route Electrical Cables, page 1-58—Complete this procedure as needed before continuing with the "NTP-A11 Install the Rear Cover" procedure on page 1-60.

13. NTP-A11 Install the Rear Cover, page 1-60—Complete this procedure as needed to install the rear cover.
14. NTP-A12 Install Ferrites, page 1-62—Complete this procedure as needed to attach ferrites to power cables.
15. NTP-A238 Install Optional DWDM Equipment, page 1-65—Complete this procedure if you are installing the optional equipment associated with DWDM applications.
16. NTP-A13 Perform the Shelf Installation Acceptance Test, page 1-67—Complete this procedure to determine if you have correctly completed all other procedures in the chapter.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning **The ONS 15454 is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock, key, or other means of security. A restricted access area is controlled by the authority responsible for the location.**

Warning **The ONS 15454 is suitable for mounting on concrete or other noncombustible surfaces only.**

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Required Tools and Equipment

You need the following tools and equipment to install and test the ONS 15454.

Cisco-Supplied Materials

The following materials are required and are shipped with the ONS 15454 shelf (wrapped in plastic). The number in parentheses gives the quantity of the item included in the package.

- #12-24 x 3/4 pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX) (8)
- #12 -24 x 3/4 socket set screws (48-1003-XX) (2)
- T-handle #12-24 hex tool for set screws (1)
- ESD wrist strap with 1.8 m (6 ft) coil cable (1)
- Tie wraps (10)
- Pinned hex (Allen) key for front door (1)
- Spacers (50-1193-XX) (4)
- Spacer mounting brackets (2)
- Clear plastic rear cover (1)
- External (bottom) brackets for the fan-tray air filter

- Standoff kit (53-0795-XX):
  - Plastic fiber management guides (2)
  - Fan filter bracket screws (53-48-0003) (6)

The following materials are required to install the optional Air Ramp. The number in parentheses gives the quantity of the item included in the package:

- M4.0x 8mm, SS pan-head Phillips mounting screws (2)
- Mounting brackets, 19-inch, 23-inch (2)

User-Supplied Materials

The following materials and tools are required but are not supplied with the ONS 15454:

- One or more of the following equipment racks:
  - 19-inch ANSI Standard (GR-63-CORE) (482.6 mm) rack; total width 22 inches (558.8 mm)
  - 23-inch ANSI Standard (GR-63-CORE) (584.2 mm) rack; total width 26 inches (660.4 mm)
- Fuse panel
- Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C])

Note If you are installing power on a 15454-SA-NEBS3E, 15454-SA-NEBS3, or 15454-SA-R1, P/N: 800-07149 shelf assembly, a #10 to #12 AWG power cable is required.

- Ground cable #6 AWG stranded

Note If you are installing power on a 15454-SA-NEBS3E, 15454-SA-NEBS3 or 15454-SA-R1, P/N: 800-07149 shelf assembly, the #10 AWG ground cable is required.

- Alarm cable pairs for all alarm connections, #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2), solid tinned
- 100-ohm shielded Building Integrated Timing Supply (BITS) clock cable pair #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2), twisted-pair T1-type
- Single-mode SC fiber jumpers with UPC polish (55 dB or better) for optical (OC-N) cards
- Shielded coaxial cable terminated with SMB or BNC connectors for DS-3 cards
- Shielded ABAM cable terminated with AMP Champ connectors or unterminated for DS1N-14 cards with #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2) ground wire (typically about two feet in length)
- 6-pair #29 AWG double-shielded cable
- Tie wraps and/or lacing cord
- Labels
- Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors

Tools Needed

- #2 Phillips screwdriver

- Medium slot-head screwdriver
- Small slot-head screwdriver
- Wire wrapper
- Wire cutters
- Wire strippers
- Crimp tool
- BNC insertion tool

Test Equipment

- Voltmeter
- Optical power meter (for use with fiber optics only)
- Bit error rate (BER) tester, DS-1 and DS-3

NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly

Purpose	This procedure unpacks the ONS 15454 and verifies the contents.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15454 high-density shelf (15454-SA-HD) is required if you want to use the high-density electrical cards (48-port DS-3 and 56-port DS-1), available in a future release.

Step 1 Complete the "DLP-A1 Unpack and Verify the Shelf Assembly" task on page 1-4.

Step 2 Complete the "DLP-A2 Inspect the Shelf Assembly" task on page 1-5.

Step 3 Continue with the "NTP-A2 Install the Shelf Assembly" procedure on page 1-6.

Stop. You have completed this procedure.

DLP-A1 Unpack and Verify the Shelf Assembly

Purpose	This task removes the shelf assembly from the package.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required

Onsite/Remote	Onsite
Security Level	None

Step 1 When you receive the ONS 15454 system equipment at the installation site, open the top of the box. The Cisco Systems logo designates the top of the box.

Step 2 Remove the foam inserts from the box. The box contains the 15454 shelf (wrapped in plastic) and a smaller box of items needed for installation.

Step 3 To remove the shelf, grasp both rings of the shelf removal strap and slowly lift the shelf out of the box.

Step 4 Open the smaller box of installation materials, and verify that you have all items listed in the "Cisco-Supplied Materials" section on page 1-2.

Note The fan-tray assembly is shipped separately.

Step 5 Return to your originating procedure (NTP).

DLP-A2 Inspect the Shelf Assembly

Purpose	This task verifies that all parts of the shelf assembly are in good condition.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	DLP-A1 Unpack and Verify the Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the shelf using the pinned hex key. For more information, see the "DLP-A8 Open the Front Door" task on page 1-13.

Step 2 Verify the following:

- Pins are not bent or broken
- Frame is not bent

Step 3 If the pins are bent or broken, or the frame is bent, call your Cisco sales engineer for a replacement.

Step 4 Close the front door before installing.

Step 5 Return to your originating procedure (NTP).

NTP-A2 Install the Shelf Assembly

Purpose	This procedure reverses the mounting bracket and mount shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Pinned hex key Two set screws (48-1003-XX)
Prerequisite Procedures	NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **To prevent the equipment from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 131°F (55°C). To prevent airflow restriction, allow at least 1 inch (25.4 mm) of clearance around the ventilation openings.**

Warning **The ONS 15454 should be installed in the lower rack position or mounted above another ONS 15454 shelf assembly.**

Warning **The ONS 15454 must have 1 inch of airspace below the installed shelf assembly to allow air flow to the fan intake. The air ramp (the angled piece of sheet metal on top of the shelf assembly) provides this spacing and should not be modified in any way.**

Note The 10 Gbps compatible shelf assembly (15454-SA-10G) and fan-tray assembly (15454-FTA3) are required with the ONS 15454 XC10G, OC-192, and OC-48 any slot (AS) cards.

Step 1 Complete the "DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack" task on page 1-7 if you need to convert from a 23-inch (584.2 mm) to a 19-inch (482.6 mm) rack.

Step 2 To install the air filter on the bottom of the shelf rather than below the fan-tray assembly, complete the "DLP-A4 Install the External Brackets and Air Filter" task on page 1-8.

Step 3 Complete the necessary rack mount task:

- DLP-A5 Mount the Shelf Assembly in a Rack (One Person), page 1-10
- DLP-A6 Mount the Shelf Assembly in a Rack (Two People), page 1-11
- DLP-A7 Mount Multiple Shelf Assemblies in a Rack, page 1-12

Step 4 Continue with the "NTP-A3 Open and Remove the Front Door" procedure on page 1-13.

Stop. You have completed this procedure.

DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack

Purpose	This task installs the mounting bracket to convert a 23-inch (584.2 mm) rack to a 19-inch (482.6 mm) rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Use only the fastening hardware provided with the ONS 15454 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15454 in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the ONS 15454 shipping kit, or remove the coating from the threads to ensure electrical continuity.

Step 1 Remove the screws that attach the mounting bracket to the side of the shelf assembly.

Step 2 Flip the detached mounting bracket upside down.

Text imprinted on the mounting bracket will now also be upside down.

Step 3 Place the widest side of the mounting bracket flush against the shelf assembly (see Figure 1-1).

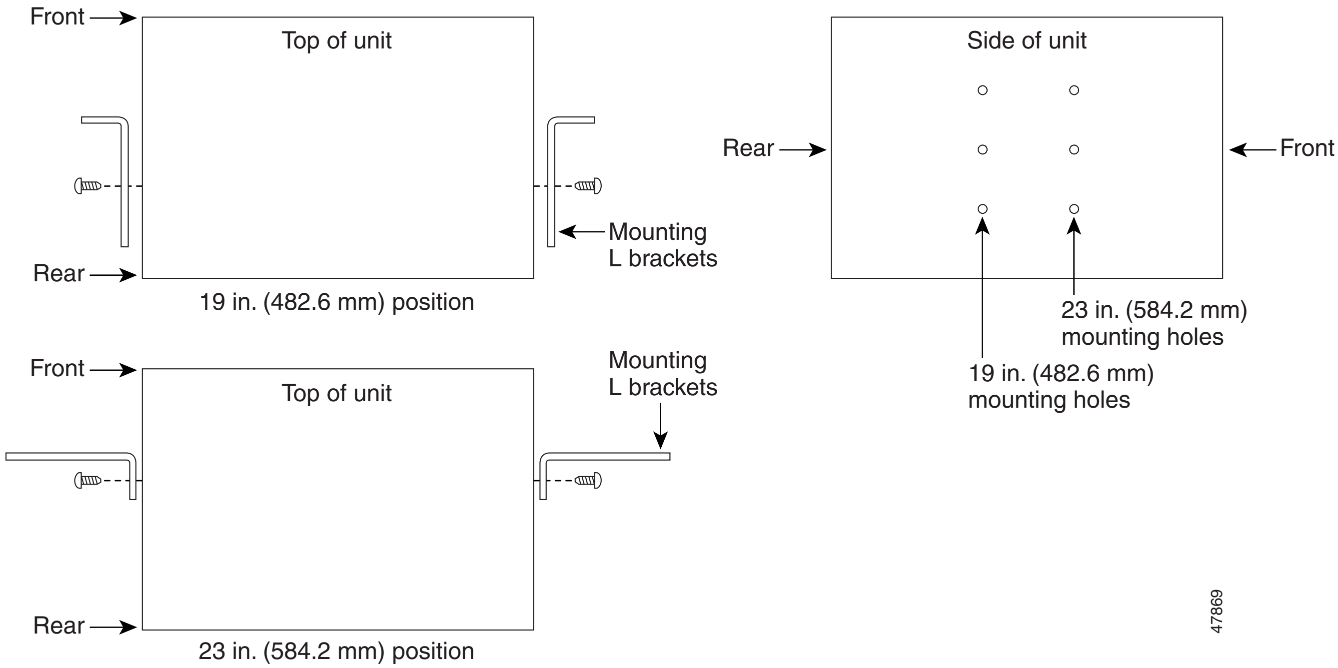
The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.

Step 4 Align the mounting bracket screw holes against the shelf assembly screw holes.

Step 5 Insert the screws that were removed in Step 1 and tighten them.

Step 6 Repeat the task for the mounting bracket on the opposite side.

Figure 1-1 Reversing the Mounting Brackets (23-inch (584.2 mm) Position to 19-inch (482.6 mm) Position)



Step 7 Return to your originating procedure (NTP).

DLP-A4 Install the External Brackets and Air Filter

Purpose	This task installs the external brackets and air filter on the bottom of the shelf rather than below the fan-tray assembly. Installing the external brackets and air filter on the bottom of the shelf enables access to the air filter without removing the fan-tray assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 1-7, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Note If you choose not to install the brackets, install the air filter by sliding it into the compartment at the bottom of the shelf assembly. Each time you remove and reinstall the air filter in the future, you must first remove the fan-tray assembly. Do not install an air filter in both filter locations on any shelf assembly.

Step 1 With the fan-tray assembly removed, place the ONS 15454 face down on a flat surface.

Note Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

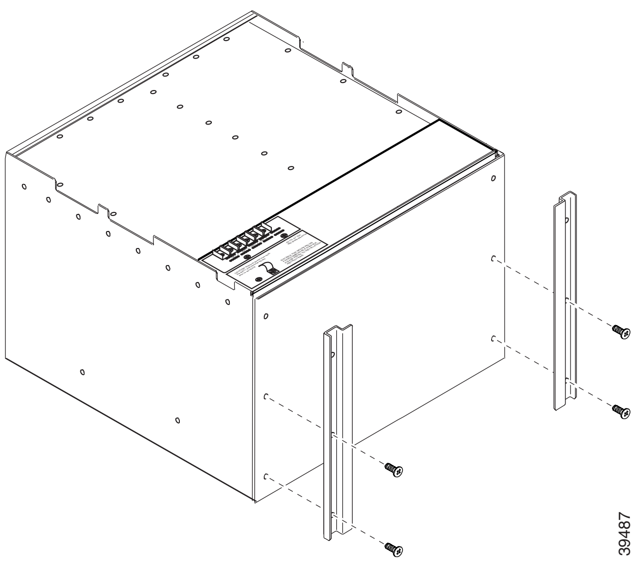
Step 2 Locate the three screw holes that run along the left and right sides of the bottom of the shelf assembly.

Step 3 Secure each bracket to the bottom of the shelf assembly using the screws (48-0003) provided in the backplane standoff kit (53-0795-XX).

Each bracket has a filter stopper and a flange on one end. Make sure to attach the brackets with the stoppers and flanges facing the rear of the shelf assembly (the top, if the ONS 15454 is face-down during installation).

Figure 1-2 illustrates bottom bracket installation. If you do not use the brackets, in the future you must remove the fan-tray assembly before removing the air filter. The brackets enable you to clean and replace the air filter without removing the fan-tray assembly.

Figure 1-2 Installing the External Brackets



Step 4 Slide the air filter into the shelf assembly.

Step 5 Return to your originating procedure (NTP).

DLP-A5 Mount the Shelf Assembly in a Rack (One Person)

Purpose	This task allows one person to mount the shelf assembly in a rack.
Tools/Equipment	Pinned hex key Two set screws (48-1003-XX) # 2 Phillips screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 1-7, if applicable DLP-A4 Install the External Brackets and Air Filter, page 1-8, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).

Step 3 Using the hex key that shipped with the assembly, install the two set screws into the screw holes that will not be used to mount the shelf.

Step 4 Lift the shelf assembly to the desired rack position and set it on the set screws.

Step 5 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6 Using the Phillips screwdriver, install one mounting screw in each side of the assembly.

Step 7 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

Step 8 Remove the temporary set screws.

Step 9 Return to your originating procedure (NTP).

DLP-A6 Mount the Shelf Assembly in a Rack (Two People)

Purpose	This task allows two people to mount the shelf assembly in a rack.
Tools/Equipment	Pinned hex key Two set screws (48-1003-XX) # 2 Phillips screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 1-7, if applicable DLP-A4 Install the External Brackets and Air Filter, page 1-8, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).

Step 3 Using the hex key that shipped with the shelf assembly, install the two set screws (48-1003-XX) into the screw holes that will not be used to mount the shelf.

Step 4 Lift the shelf assembly to the desired position in the rack.

Step 5 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6 While one person holds the shelf assembly in place, the other person can install one mounting screw in each side of the assembly using the Phillips screwdriver.

Step 7 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

Step 8 Remove the temporary set screws.

Step 9 Return to your originating procedure (NTP).

DLP-A7 Mount Multiple Shelf Assemblies in a Rack

Purpose	This task allows multiple shelves to be assembled in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 1-7, if applicable DLP-A4 Install the External Brackets and Air Filter, page 1-8, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15454 must have one inch (25.4 mm) of airspace below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 is installed underneath a shelf assembly, the air ramp on top of the bottom shelf assembly provides the desired space. However, if the ONS 15454 is installed above third-party equipment, you must provide a minimum spacing of one inch (25.4 mm) between the third-party shelf assembly and the bottom of the ONS 15454. The third-party equipment must not vent heat upward into the ONS 15454.

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer's instructions.

- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

Step 2 Mount the first ONS 15454 directly below the fuse and alarm panel using the "DLP-A5 Mount the Shelf Assembly in a Rack (One Person)" task on page 1-10 or the "DLP-A6 Mount the Shelf Assembly in a Rack (Two People)" task on page 1-11.

Step 3 Repeat the task with the remaining shelves.

Step 4 Return to your originating procedure (NTP).

NTP-A3 Open and Remove the Front Door

Purpose	This procedure opens and removes the front door to access the equipment.
Tools/Equipment	Open-end wrench Pinned hex key
Prerequisite Procedures	NTP-A2 Install the Shelf Assembly, page 1-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A8 Open the Front Door" task on page 1-13.

Step 2 As needed, complete the "DLP-A9 Remove the Front Door" task on page 1-14.

Step 3 Continue with the "NTP-A4 Remove the Backplane Covers" procedure on page 1-16.

Stop. You have completed this procedure.

DLP-A8 Open the Front Door

Purpose	This task describes how to open the front cabinet compartment door.
Tools/Equipment	Pinned hex key
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Note The ONS 15454 has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside edge of the shelf assembly on the right-hand side. It is labeled "ESD" on the top and bottom. Always wear an ESD wrist strap and connect the strap to the ESD plug when working on the ONS 15454.

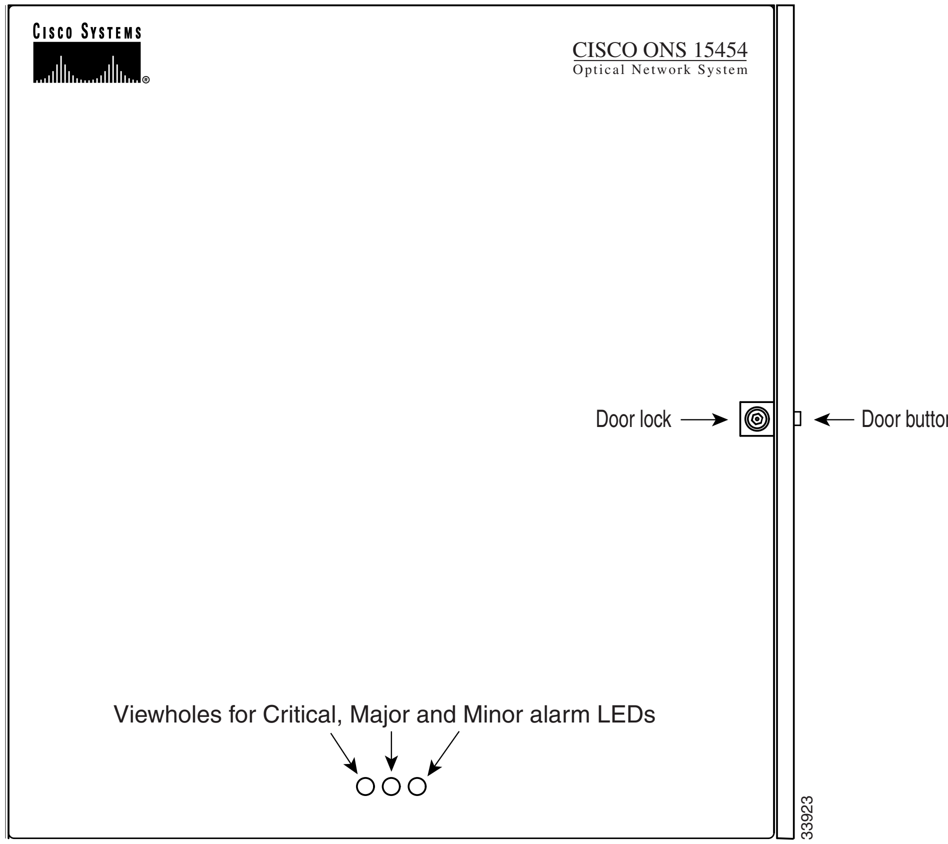
Step 1 Open the front door lock (Figure 1-3).

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.

Step 2 Press the door button to release the latch.

Step 3 Swing the door open.

Figure 1-3 Cisco ONS 15454 Front Door



Step 4 Return to your originating procedure (NTP).

DLP-A9 Remove the Front Door

Purpose	Use this task to remove the front cabinet compartment door.
Tools/Equipment	Open-end wrench
Prerequisite Procedures	DLP-A8 Open the Front Door, page 1-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

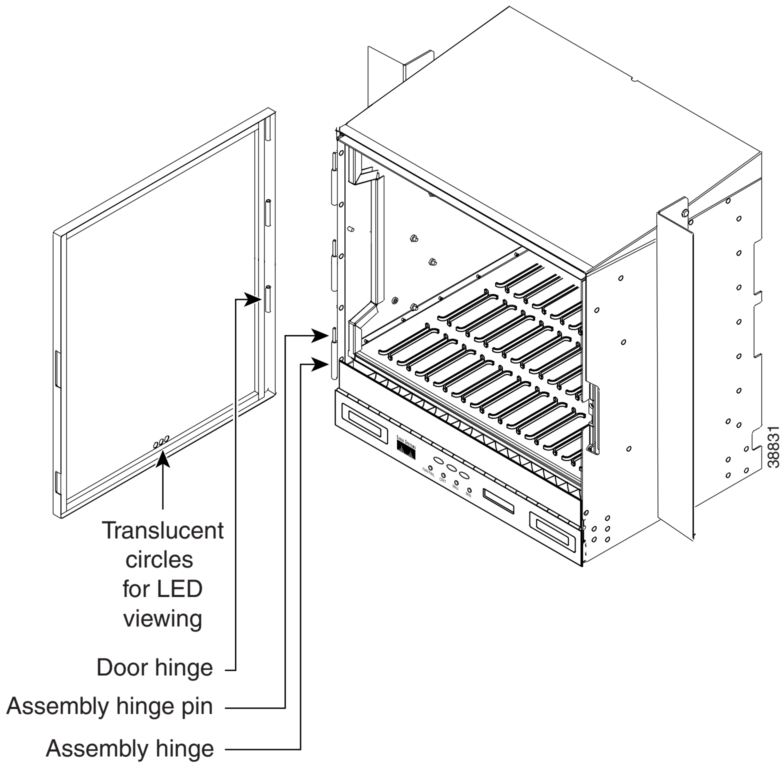
Step 1 To remove the door ground strap (available in Release 3.3 and later), perform the following:

a. To detach the ground strap from the front door, loosen the #6 kep nut (49-0600-01) using the open-end wrench. Detach the end of the ground strap terminal lug (72-3622-01) from the male stud on the inside of the door.

b. To detach the other end of the ground strap from the longer screw on the fiber guide, loosen the #4 kep nut (49-0337-01) on the terminal lug using the open-end wrench. Remove the terminal lug and lock washer.

Step 2 Lift the door from its hinges at the top left corner of the door (Figure 1-4).

Figure 1-4 Removing the ONS 15454 Front Door



Step 3 Return to your originating procedure (NTP).

NTP-A4 Remove the Backplane Covers

Purpose	This procedure describes how to access the backplane by removing the covers. The backplane has two sheet metal covers (one on either side) and a lower backplane cover at the bottom.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-13 NTP-A2 Install the Shelf Assembly, page 1-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A10 Remove the Lower Backplane Cover" task on page 1-16.

Step 2 Complete the "DLP-A11 Remove the Backplane Sheet Metal Cover" task on page 1-17.

Step 3 If you plan to install electrical interface assemblies (EIAs), continue with the "NTP-A5 Install the EIAs" procedure on page 1-17. If not, continue with the "NTP-A6 Install the Power and Ground" procedure on page 1-25.

Stop. You have completed this procedure.

DLP-A10 Remove the Lower Backplane Cover

Purpose	This task removes the lower backplane cover.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Unscrew the five retaining screws that hold the clear plastic cover in place.

Step 2 Grasp the clear plastic cover on each side.

Step 3 Gently pull the cover away from the backplane.

Step 4 Return to your originating procedure (NTP).

DLP-A11 Remove the Backplane Sheet Metal Cover

Purpose	This task removes the backplane sheet cover that is installed on the backplane when EIAs are not installed.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 1-16
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 To remove the lower clear plastic backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover(s) in place.

Step 3 Lift the panel by the bottom to remove it from the shelf assembly.

Step 4 Store the panel for later use. Attach the backplane cover(s) whenever EIA(s) are not installed.

Step 5 Return to your originating procedure (NTP).

NTP-A5 Install the EIAs

Purpose	This procedure describes how to install electrical interface assemblies (EIAs). Typically an EIA panel is installed on the backplane during manufacturing, but EIA panels can be ordered separately. Refer to the *Cisco ONS 15454 Reference Manual* for descriptions of the EIAs.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Perimeter screws (9) Inner screws (12) Backplane cover screws (5) EIA card (SMB, BNC, AMP Champ)
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-16
Required/As Needed	Required if the node will use electrical signals
Onsite/Remote	Onsite
Security Level	None

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 EIAs are normally factory installed. Verify that the correct EIA is installed on the shelf assembly. If not, install the correct EIA.

Note You do not need to power down the shelf before removing or installing an EIA. An in-service upgrade of one EIA (A side or B side) is possible if all electrical traffic (DS-1, DS-3, DS3XM-6, and EC-1) is being carried on the other side.

Step 1 Complete the "DLP-A12 Install a BNC or High-Density BNC EIA" task on page 1-19 as needed. BNCs are locking connectors; the high-density BNC provides access to every port on every card.

Step 2 Complete the "DLP-A13 Install an SMB EIA" task on page 1-22 as needed. SMBs allow you to access every port on every card using more space and efficient cabling.

Step 3 Complete the "DLP-A14 Install the AMP Champ EIA" task on page 1-23 as needed. AMP Champs are exclusive to DS-1 cables.

Note To attach cables to the EIAs, see the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-49.

Step 4 Continue with the "NTP-A6 Install the Power and Ground" procedure on page 1-25.

Stop. You have completed this procedure.

DLP-A12 Install a BNC or High-Density BNC EIA

Purpose	This task installs a BNC or high-density BNC EIA. Use this task if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer a BNC interface to an SMB interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Perimeter screws (9) Inner screws (12) Backplane cover screws (5) BNC or high-density BNC card
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the BNC or high-density BNC card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.

Step 2 Place the metal EIA panel over the card.

Step 3 Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb. (3.6 to 4.5 kg) to secure the cover panel to the backplane.

Step 4 Insert and tighten the twelve (BNC) or nine (high-density BNC) inner screws (P/N 48-0004) at 8 to 10 lb. (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.

Figure 1-5 shows a BNC EIA installation.

Figure 1-5 Installing the BNC EIA

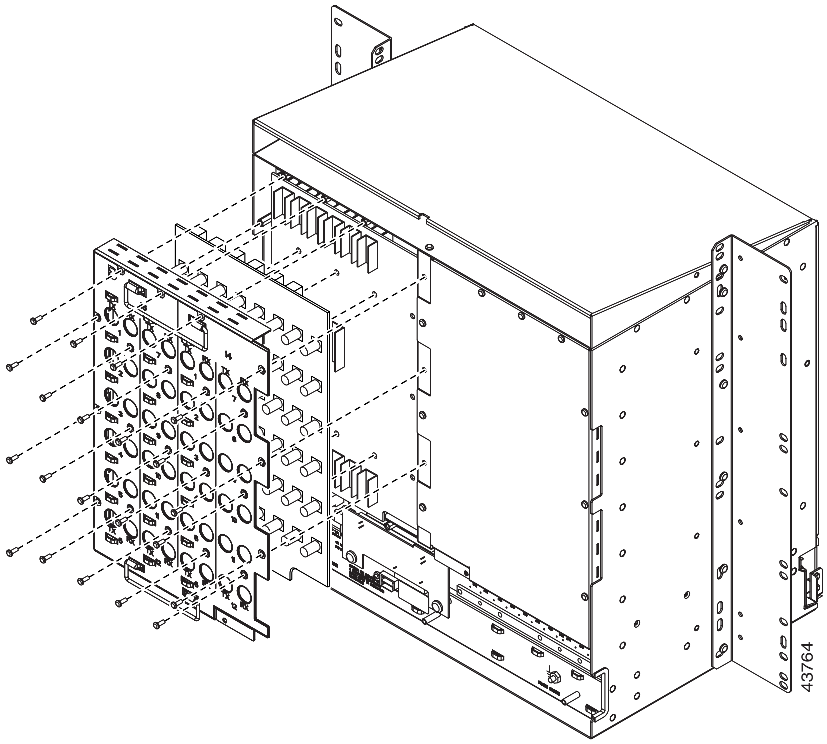
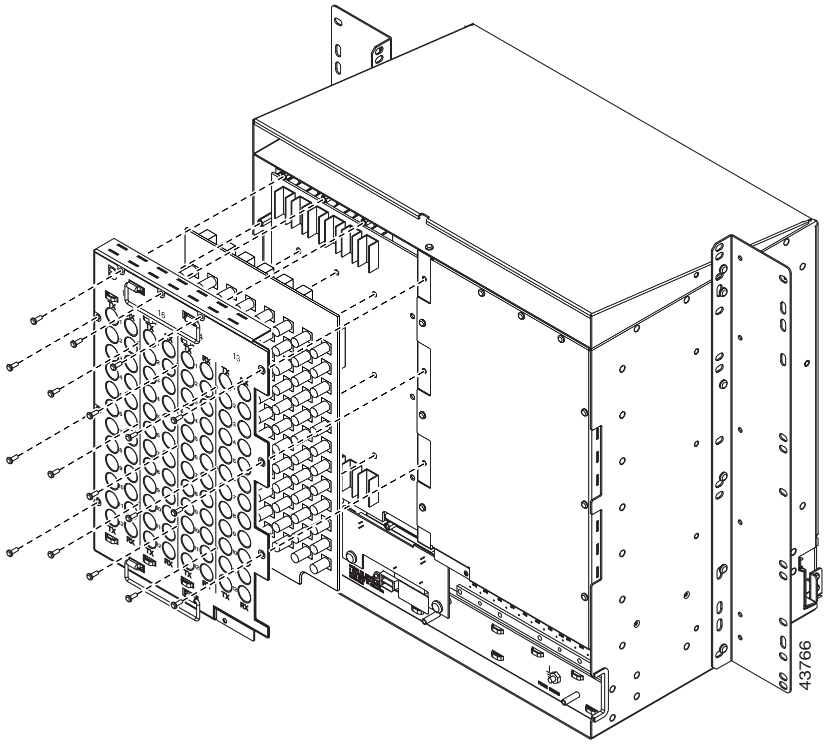


Figure 1-6 shows high-density BNC EIA installation.

Figure 1-6 Installing the High-Density BNC EIA



Step 5 Return to your originating procedure (NTP).

DLP-A13 Install an SMB EIA

Purpose	This task installs an SMB EIA. Use the SMB EIA if you are using DS1-14 cards and prefer an SMB interface to an AMP interface, or if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer an SMB interface to a BNC interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws SMB card EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed.**

Step 1 Remove the SMB card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.

Step 2 Place the EIA panel over the card.

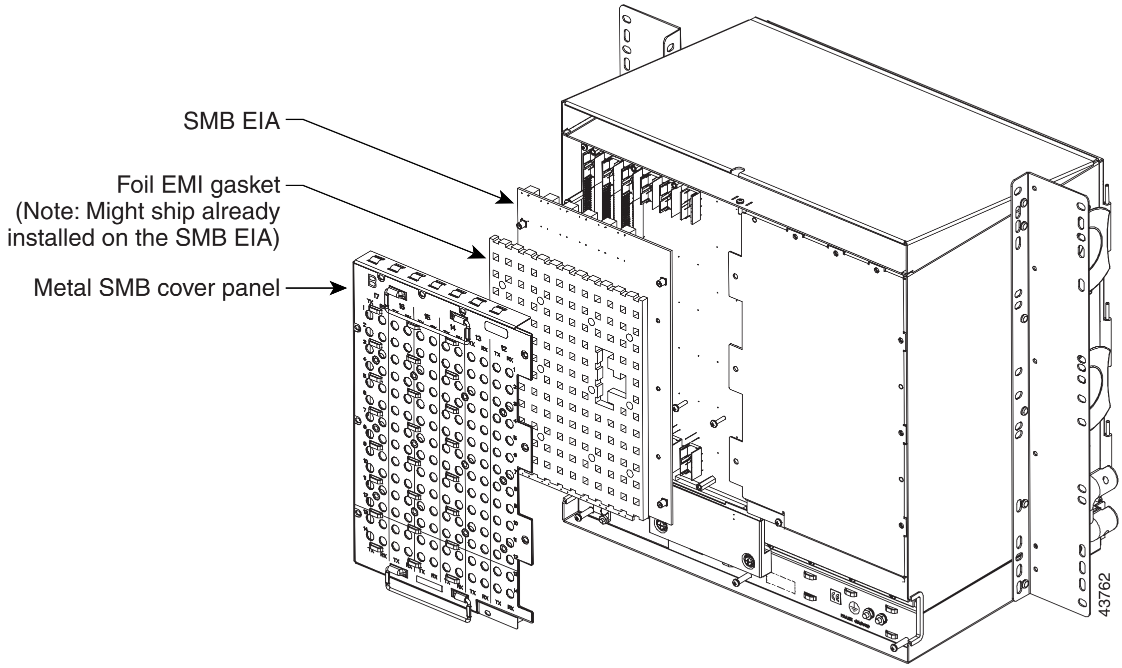
Step 3 Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb. (3.6 to 4.5 kg) to secure the cover panel to the backplane.

Step 4 Insert and tighten the twelve inner screws (P/N 48-0004) at 8 to 10 lb. (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.

If you are using SMB EIAs to make DS-1 connections, you need the DS-1 electrical interface adapter, commonly referred to as a balun (P/N 15454-WW-14=).

Figure 1-7 on page 1-23 shows an SMB EIA installation.

Figure 1-7 Installing the SMB EIA (Use a Balun for DS-1 Connections)



Step 5 Return to your originating procedure (NTP).

DLP-A14 Install the AMP Champ EIA

Purpose	This task installs an AMP Champ EIA. Use an AMP Champ EIA if you are using DS1-14 cards and prefer an AMP interface to an SMB interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws 6 AMP Champ cards EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the AMP Champ panel with the backplane and insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb. (3.6 to 4.5 kg).

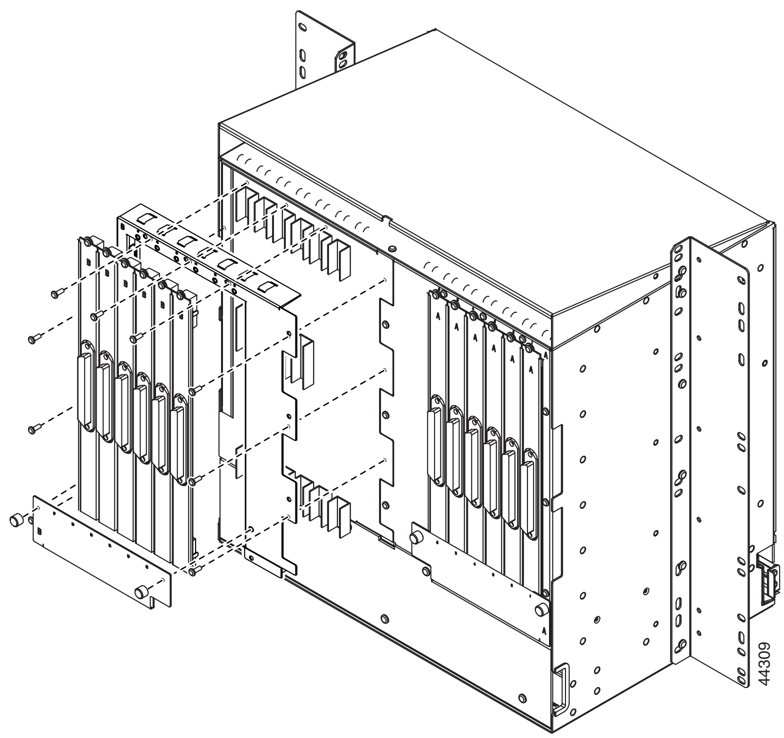
Step 2 Align an AMP Champ card with the backplane connector and push until it fits snugly. Repeat until you have installed all six AMP Champ cards.

Step 3 To secure each AMP Champ card to the cover panel, insert and tighten a screw (P/N 48-0003) at the top of each card at 8 to 10 lb. (3.6 to 4.5 kg).

Step 4 Place the AMP Champ fastening plate along the bottom of the cover panel, and hand-tighten the two thumbscrews.

Figure 1-8 shows an AMP Champ EIA installation.

Figure 1-8 Installing the AMP Champ EIA



Step 5 Return to your originating procedure (NTP).

NTP-A6 Install the Power and Ground

Purpose	This procedure installs power feeds and ground the ONS 15454.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors Wire wrapper Wire cutters Wire strippers Crimp tool Fuse panel
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-16
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Shut off the power from the power source or turn off the breakers before beginning work.**

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Warning **Do not mix conductors of dissimilar metals in a terminal or splicing connector where physical contact occurs (such as copper and aluminum, or copper and copper-clad aluminum), unless the device is suited for the purpose and conditions of use.**

Warning **Connect the ONS 15454 only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950-based safety standards.**

Warning **The ONS 15454 relies on the protective devices in the building installation to protect against short circuit, overcurrent, and grounding faults. Ensure that the protective devices are properly rated to protect the system, and that they comply with national and local codes.**

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.**

Warning **When installing redundant power feeds, do not use aluminum conductors.**

Warning **If you use redundant power leads to power the ONS 15454, disconnecting one lead will not remove power from the node.**

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.

Step 1 Verify one of the following:

- If you have the 15454-SA-ANSI or 15454-SA-HD shelf, a 100-A fuse panel (30-A fuse per shelf minimum) should be installed. If not, install one according to manufacturer's instructions.
- If you have the 15454-SA-NEBS3 shelf, a standard 80-A fuse panel (20-A fuse per shelf minimum) should be installed. If not, install one according to manufacturer's instructions.

Step 2 Complete the "DLP-A16 Connect the Office Ground to the ONS 15454" task on page 1-27.

Step 3 Complete the "DLP-A17 Connect Office Power to the ONS 15454 Shelf" task on page 1-28.

Step 4 Complete the "DLP-A18 Turn On and Verify Office Power" task on page 1-30.

Step 5 Continue with the "NTP-A7 Install the Fan-Tray Assembly" procedure on page 1-31.

Stop. You have completed this procedure.

DLP-A16 Connect the Office Ground to the ONS 15454

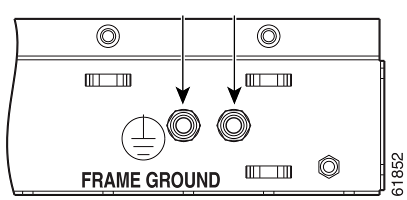
Purpose	This task connects ground to the ONS 15454 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 1-16
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the office ground cable (#6 AWG stranded) is connected to the top of the bay according to local site practice.

Step 2 Attach one end of the shelf ground cable (#10 AWG) to the right side of the backplane ground nut. See Figure 1-9 for the location of the ground on the backplane.

Note When terminating a frame ground, use the kep nut provided with the ONS 15454 and tighten it to a torque specification of 31 in-lb. The kep nut provides a frame ground connection that minimizes the possibility of loosening caused by rotation during installation and maintenance activity. The type of prevention the kep nut provides for the frame ground connection is inherently provided by the terminal block for battery and battery return connections.

Figure 1-9 Ground Location on the Backplane



Step 3 Attach the other end of the shelf ground cable to the bay.

Step 4 Return to your originating procedure (NTP).

DLP-A17 Connect Office Power to the ONS 15454 Shelf

Purpose	This task connects power to the ONS 15454 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Wire cutters Wire strippers Crimp tool Fuse panel Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors
Prerequisite Procedures	DLP-A16 Connect the Office Ground to the ONS 15454, page 1-27
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Do not apply power to the ONS 15454 until you complete all installation steps and check the continuity of the -48 VDC and return.**

Note The battery return connection is treated as DC-I, as defined in GR-1089-CORE Issue 3.

Note If the system loses power or both TCC2 cards are reset and the system is not provisioned to get the time from a Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server, you must reset the ONS 15454 clock. After powering down, the date defaults to January 1, 1970, 00:04:15. To reset the clock, see the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-7. If you are using the TCC2 cards, the system clock will be kept running for up to three hours. In this case, no action would be required.

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

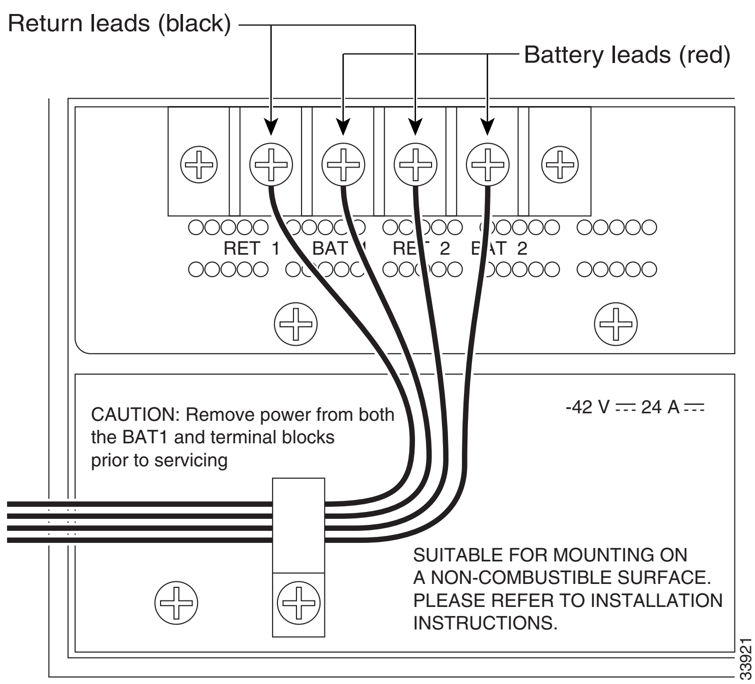
Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15454 from the fuse panel. Figure 1-10 shows the ONS 15454 power terminals.

Step 3 Dress the power according to local site practice.

Warning **When installing the ONS 15454, the ground connection must always be made first and disconnected last.**

Figure 1-10 Cisco ONS 15454 Power Terminals



Step 4 Remove or loosen the #8 power terminal screws on the ONS 15454. To avoid confusion, label the cables connected to the BAT1/RET1 (A) power terminals as 1, and the cables connected to the BAT2/RET2 (B) power terminals as 2.

Note Use only pressure terminal connectors, such as ring and fork types, when terminating the battery, battery return, and frame ground conductors.

Caution Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.

Caution When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

Step 5 Strip 1/2 inch (12.7 mm) of insulation from all power cables that you will use.

Step 6 Crimp the lugs onto the ends of all power leads.

Note When terminating battery and battery return connections as shown in Figure 1-10, follow a torque specification of 10 in-lb.

Step 7 Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections noncorrosive.

Warning **Do not secure multiple connectors with the same bolt assembly.**

Step 8 Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections noncorrosive.

Step 9 If you use redundant power leads, terminate the return 2 lead to the positive RET2 terminal on the ONS 15454. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15454. Use oxidation-preventative grease to keep connections noncorrosive.

Step 10 Route the cables out below the power terminals using the plastic cable clamp, as shown in Figure 1-10 on page 1-29.

Step 11 Return to your originating procedure (NTP).

DLP-A18 Turn On and Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-A16 Connect the Office Ground to the ONS 15454, page 1-27
	DLP-A17 Connect Office Power to the ONS 15454 Shelf, page 1-28
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:

a. To verify the power, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side connection and verify that it is between –40.5 VDC and –57 VDC. Place the red test lead on the B-side connection and verify that it is between –40.5 VDC and –57 VDC.

Note The voltages –40.5 VDC and –57 VDC are, respectively, the minimum and maximum voltages required to power the chassis.

b. To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side return ground and verify that no voltage is present. Place the red test lead on the B-side return ground and verify that no voltage is present.

Step 2 Complete one of the following to power up the node:

- If you are using a 80-A fuse panel, insert a 20-A fuse into the fuse position according to site practice.

- If you are using a 100-A fuse panel, insert a 30-A fuse into the fuse position according to site practice.

Step 3 Using a voltmeter, verify the shelf for –48 VDC battery and ground:

a. To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify that it reads between –40.5 VDC and –57 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

Note The voltages –40.5 VDC and –57 VDC are, respectively, the minimum and maximum voltages required to power the chassis.

b. To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify that it reads between –40.5 VDC and –57 VDC. Then, place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

Step 4 Return to your originating procedure (NTP).

NTP-A7 Install the Fan-Tray Assembly

Purpose	This procedure installs the fan-tray assembly.
Tools/Equipment	#2 Phillips screwdriver
	Medium slot-head screwdriver
	Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-13
	NTP-A6 Install the Power and Ground, page 1-25
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution Do not operate an ONS 15454 without a fan-tray air filter. A fan-tray air filter is mandatory in order to comply with GR-78-CORE, except for applications in an outside plant cabinet.

Note If you are installing the ONS 15454 in an outside plant cabinet, remove the air filter to provide maximum cooling capabilities and to comply with GR-487-CORE.

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 or later shelf assemblies (15454-SA-ANSI, 800-19857; 15454-SA-HD, 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released earlier than ONS 15454 Release 3.1

(15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N 800-0714915454). Installing the 15454-FTA3 in a noncompliant shelf assembly might result in failure of the alarm interface panel (AIP), which in turn, will result in power loss to the fan-tray assembly.

Caution You must place the edge of the air filter flush against the front of the fan-tray assembly compartment when installing the fan tray on top of the filter. Failure to do so could result in damage to the filter, the fan tray, or both.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.

Note To install the fan-tray assembly, it is not necessary to move any of the cable-management facilities.

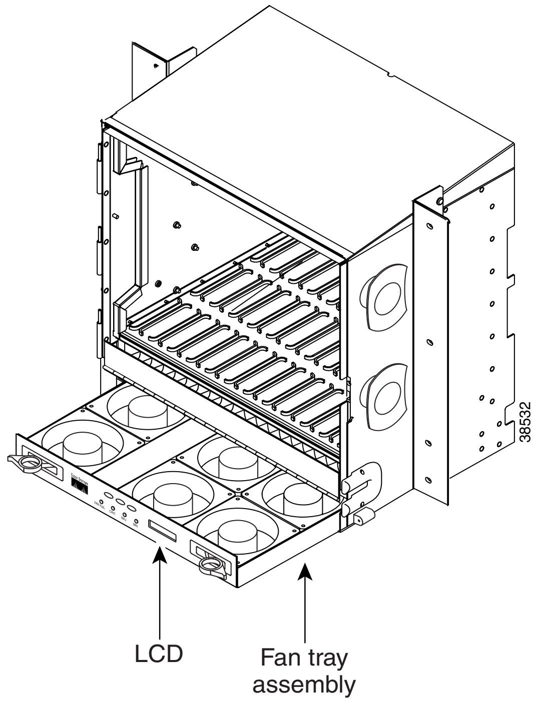
Step 1 Install the air filter. The air filter can be installed internally between the fan tray and shelf assembly, or externally by mounting the air filter bracket on the bottom of the shelf assembly. Slide the air filter into the bracket.

Step 2 Slide the 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 3 To verify that the tray has plugged into the backplane, look at the fan tray and listen to determine that the fans are running.

Figure 1-11 shows the location of the fan tray.

Figure 1-11 Installing the Fan-Tray Assembly



Step 4 Continue with the "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-34 if you plan to install an Alarm Expansion Panel (AEP). If not, continue with the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-37.

Stop. You have completed this procedure.

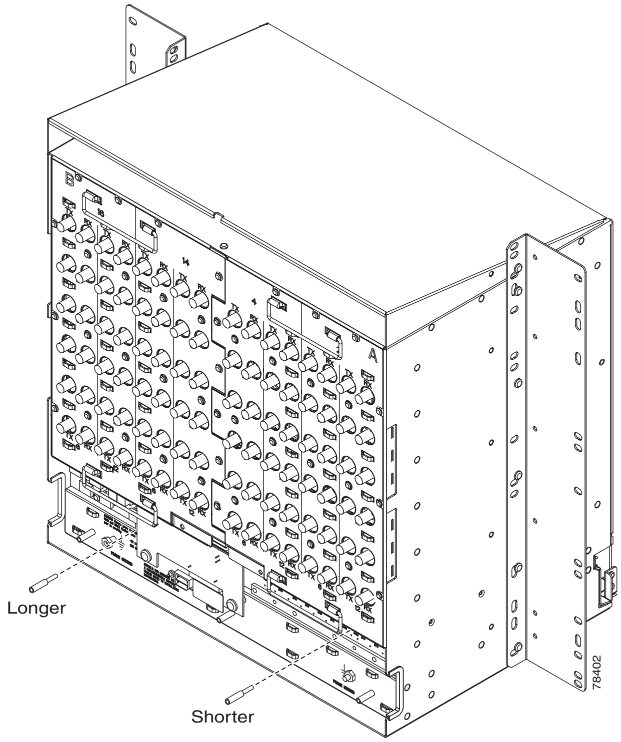
NTP-A119 Install the Alarm Expansion Panel

Purpose	This procedure installs an alarm expansion panel (AEP) onto the 15454-SA-ANSI or 15454-SA-HD shelf backplane. The AEP provides alarm contacts in addition to the 16 provided by the AIC-I card. Typically, the AEP is pre-installed when ordered with the ONS 15454; however, the AEP can be ordered separately. The AIC-I card must be installed before you can provision the alarm contacts enabled by the AEP.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper 6-pair #29 AWG double-shielded cable Standoffs (4)
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 1-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The AIC-I card provides direct alarm contacts (external alarm inputs and external control outputs). In the ANSI shelf, these AIC-I alarm contacts are routed through the backplane to wire-wrap pins accessible from the back of the shelf. When you install an AEP, the direct AIC-I alarm contacts cannot be used. Only the AEP alarm contacts can be used.

Step 1 Remove the two backplane screws. Replace the two screws with standoffs. Insert the longer standoff on the left, and the shorter standoff on the right (Figure 1-12).

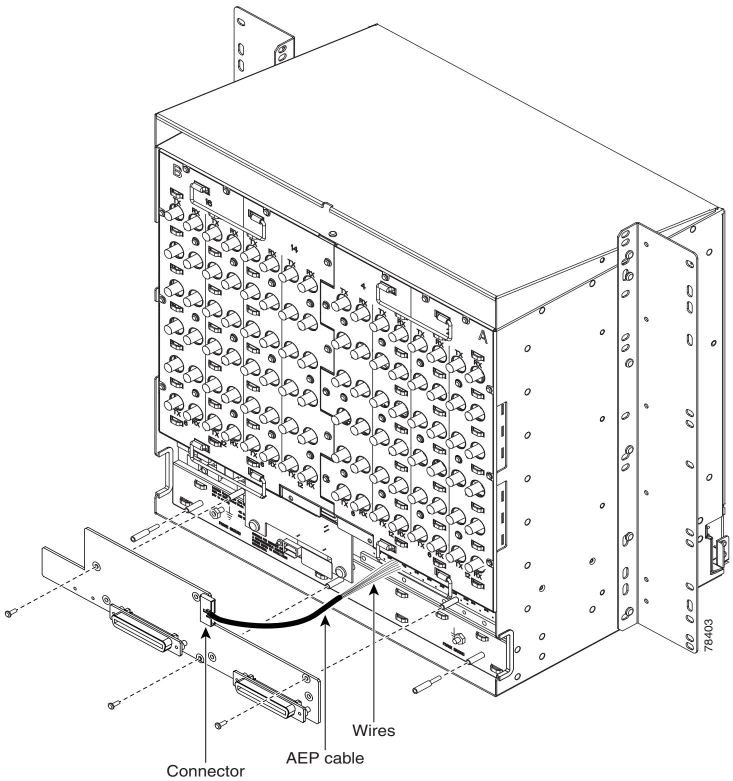
Figure 1-12 Replace Backplane Screws with Standoffs



Step 2 Attach the remaining two standoffs on either side of the backplane (Figure 1-13).

Step 3 Position the AEP board over the standoffs.

Figure 1-13 Installing Standoffs and the AEP



Step 4 Insert and tighten three screws to secure the AEP to the backplane.

Step 5 Connect the AEP cable to the backplane and AEP:

a. Connect the 10 colored wires to the wire-wrap pins on the backplane. Figure 1-14 shows where the cable wires are connected. Table 1-1 shows AEP and AIC-I signals that each wire carries.

b. Plug the other end of the AEP cable into AEP connector port. The brown pin is on the top.

Figure 1-14 AEP Wire-Wrap Connections to Backplane Pins

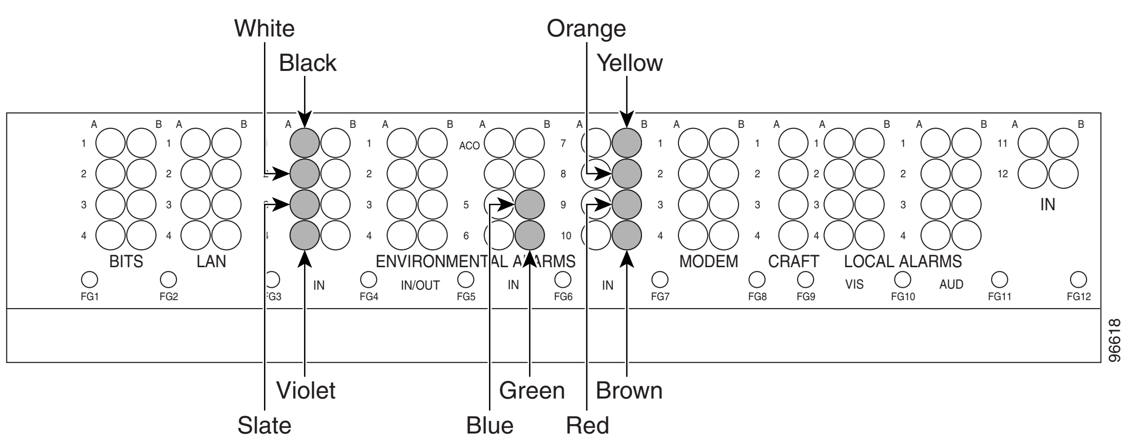


Table 1-1 Pin Assignments for the AEP

AEP Cable Wire	Backplane Pin	AIC-I Signal	AEP Signal
Black	A1	GND	AEP_GND
White	A2	AE_+5	AEP_+5
Slate	A3	VBAT-	VBAT-
Violet	A4	VB+	VB+
Blue	A5	AE_CLK_P	AE_CLK_P
Green	A6	AE_CLK_N	AE_CLK_N
Yellow	A7	AE_DIN_P	AE_DOUT_P
Orange	A8	AE_DIN_N	AE_DOUT_N
Red	A9	AE_DOUT_P	AE_DIN_P
Brown	A10	AE_DOUT_N	AE_DIN_N

Step 6 Continue with the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-37.

Stop. You have completed this procedure.

NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections

Purpose	This procedure describes how to install alarm, timing, LAN, and craft wires.
Tools/Equipment	Wire wrapper
	#22 or #24 AWG (0.51 mm² or 0.64 mm²) alarm wires
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A19 Install Alarm Wires on the Backplane" task on page 1-38 if you are using an AIC or AIC-I card and are not using an AEP.

Step 2 Complete the "DLP-A20 Install Timing Wires on the Backplane" task on page 1-41 as needed. Timing wires are necessary to provision external timing.

Step 3 Complete the "DLP-A21 Install LAN Wires on the Backplane" task on page 1-42 as needed. LAN wires (or the LAN port on the TCC2) are necessary to create an external LAN connection.

Step 4 Complete the "DLP-A22 Install the TL1 Craft Interface" task on page 1-43 as needed. Craft wires (or the EIA/TIA-232 port on the TCC2) are required to access TL1 using the craft interface.

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.

Step 5 Complete one of the following:

- If you installed an alarm expansion panel (AEP), continue with the "NTP-A120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-44.
- If you did not install an AEP and you plan to install electrical cards, continue with the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-49.
- If you did not install an AEP and do not plan to install electrical cards, continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-60.

Stop. You have completed this procedure.

DLP-A19 Install Alarm Wires on the Backplane

Purpose	This task installs alarm wires on the backplane so that you can provision external (environmental) alarms and controls with the AIC or AIC-I card. If you are using the AEP, do not perform this task.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) wires 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

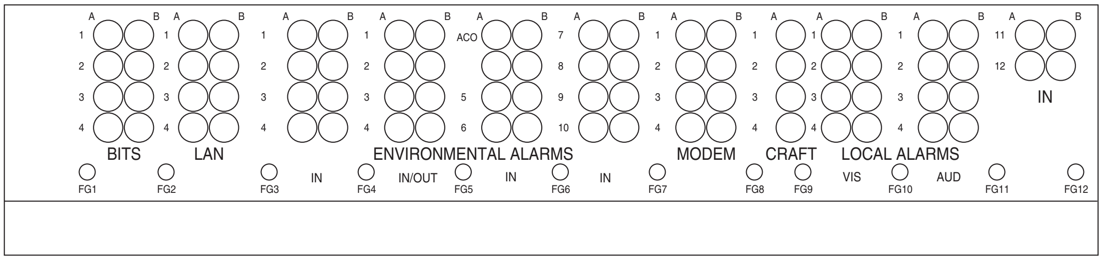
Step 1 Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²) twisted-pair T1-type wires, wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Ground the shield of the BITS Input cable at the BITS end. For BITS Output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located below the column of BITS Pins.

Figure 1-15 shows alarm pin assignments for the AIC-I in the Release 3.4 or higher ONS 15454 backplane and Figure 1-16 calls out the environmental alarm pins onthat backplane. Figure 1-17 shows alarm pin assignments for the AIC in a shelf for Release 3.3 and earlier.

Note The AIC-I requires a shelf assembly running Software Release 3.4.0 or later. The backplane of the ANSI shelf contains a wire-wrap field with pin assignment according to the layout in Figure 1-15. The shelf assembly may be an existing shelf that has been upgraded to 3.4. In this case the backplane pin labeling will appear as indicated in Figure 1-17 on page 1-40 but you must use the pin assignments provided by the AIC-I as shown in Figure 1-15.

For information about attaching ferrites to wire-wrap pin fields, see the "DLP-A31 Attach Ferrites to Wire-Wrap Pin Fields" task on page 1-64.

Figure 1-15 Cisco ONS 15454 Backplane Pinouts (Release 3.4 or Later)



Field	Pin	Function
BITS	A1	BITS Output 2 negative (–)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (–)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (–)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (–)
	B4	BITS Input 1 positive (+)
LAN		Connecting to a hub, or switch
	A1	RJ-45 pin 6 RX–
	B1	RJ-45 pin 3 RX+
	A2	RJ-45 pin 2 TX–
	B2	RJ-45 pin 1 TX+
		Connecting to a PC/Workstation or router
	A1	RJ-45 pin 2 RX–
	B1	RJ-45 pin 1 RX+
	A2	RJ-45 pin 6 TX–
	B2	RJ-45 pin 3 TX+
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.
	B1	
	A2	Alarm input pair number 2: Reports closure on connected wires.
	B2	
	A3	Alarm input pair number 3: Reports closure on connected wires.
	B3	
	A4	Alarm input pair number 4: Reports closure on connected wires.
	B4	
	A5	Alarm input pair number 5: Reports closure on connected wires.
	B5	
	A6	Alarm input pair number 6: Reports closure on connected wires.
	B6	
	A7	Alarm input pair number 7: Reports closure on connected wires.
	B7	
	A8	Alarm input pair number 8: Reports closure on connected wires.
	B8	
	A9	Alarm input pair number 9: Reports closure on connected wires.
	B9	
	A10	Alarm input pair number 10: Reports closure on connected wires.
	B10	
	A11	Alarm input pair number 11: Reports closure on connected wires.
	B11	
	A12	Alarm input pair number 12: Reports closure on connected wires.
	B12	

Field	Pin	Function
ENVIR ALARMS IN/OUT N/O	A1/A13	Normally open output pair number 1
	B1/B13	
	A2/A14	Normally open output pair number 2
	B2/B14	
	A3/A15	Normally open output pair number 3
	B3/B15	
	A4/A16	Normally open output pair number 4
	B4/B16	
ACO	A1	Normally open ACO pair
	B1	
CRAFT	A1	Receive (PC pin #2)
	A2	Transmit (PC pin #3)
	A3	Ground (PC pin #5)
	A4	DTR (PC pin #4)
LOCAL ALARMS AUD (Audible) N/O	A1	Alarm output pair number 1: Remote audible alarm.
	B1	
	A2	Alarm output pair number 2: Critical audible alarm.
	B2	
	A3	Alarm output pair number 3: Major audible alarm.
	B3	
	A4	Alarm output pair number 4: Minor audible alarm.
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	Alarm output pair number 1: Remote visual alarm.
	B1	
	A2	Alarm output pair number 2: Critical visual alarm.
	B2	
	A3	Alarm output pair number 3: Major visual alarm.
	B3	
	A4	Alarm output pair number 4: Minor visual alarm.
	B4	

If you are using an AIC-I card, contacts provisioned as OUT are 1-4. Contacts provisioned as IN are 13-16.

83020

Figure 1-16 Highlighted Environmental Alarms

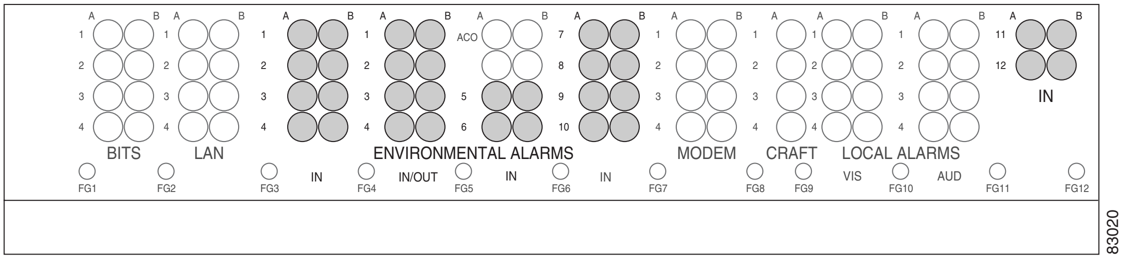
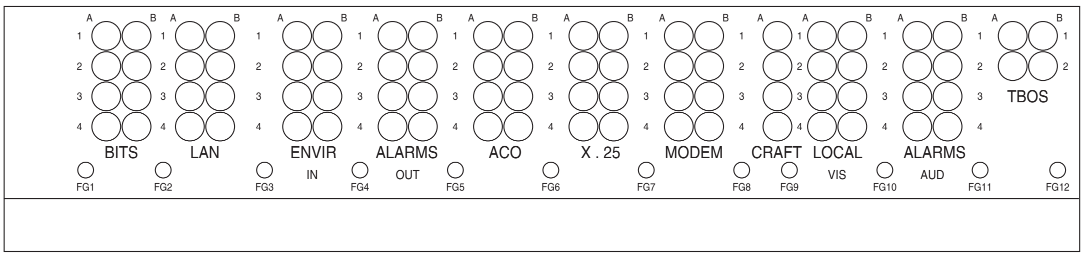


Figure 1-17 Cisco ONS 15454 Backplane Pinouts (Release 3.3 or Earlier)



Field	Pin	Function
BITS	A1	BITS Output 2 negative (-)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (-)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (-)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (-)
	B4	BITS Input 1 positive (+)
LAN	Connecting to a hub, or switch	
	A1	RJ-45 pin 6 RX-
	B1	RJ-45 pin 3 RX+
	A2	RJ-45 pin 2 TX-
	B2	RJ-45 pin 1 TX+
	Connecting to a PC/Workstation or router	
	A1	RJ-45 pin 2 RX-
	B1	RJ-45 pin 1 RX+
	A2	RJ-45 pin 6 TX-
	B2	RJ-45 pin 3 TX+
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.
	B1	
	A2	Alarm input pair number 2: Reports closure on connected wires.
	B2	
	A3	Alarm input pair number 3: Reports closure on connected wires.
	B3	
	A4	Alarm input pair number 4: Reports closure on connected wires.
	B4	

Field	Pin	Function
ENVIR ALARMS OUT N/O	A1	Normally open output pair number 1
	B1	
	A2	Normally open output pair number 2
	B2	
	A3	Normally open output pair number 3
	B3	
	A4	Normally open output pair number 4
	B4	
ACO	A1	Normally open ACO pair
	B1	
CRAFT	A1	Receive (PC pin #2)
	A2	Transmit (PC pin #3)
	A3	Ground (PC pin #5)
	A4	DTR (PC pin #4)
LOCAL ALARMS AUD (Audible) N/O	A1	Alarm output pair number 1: Remote audible alarm.
	B1	
	A2	Alarm output pair number 2: Critical audible alarm.
	B2	
	A3	Alarm output pair number 3: Major audible alarm.
	B3	
	A4	Alarm output pair number 4: Minor audible alarm.
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	Alarm output pair number 1: Remote visual alarm.
	B1	
	A2	Alarm output pair number 2: Critical visual alarm.
	B2	
	A3	Alarm output pair number 3: Major visual alarm.
	B3	
	A4	Alarm output pair number 4: Minor visual alarm.
	B4	

38533

Note The X.25, Modem, and TBOS pin fields are not active on either pin field.

Step 2 Return to your originating procedure (NTP).

DLP-A20 Install Timing Wires on the Backplane

Purpose	This task installs the BITS timing wires on the backplane.
Tools/Equipment	Wire wrapper 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type, wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Ground the shield of the BITS input cable at the BITS end. For BITS output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located beneath the column of BITS Pins. Table 1-2 lists the pin assignments for the BITS timing pin fields.

Table 1-2 External Timing Pin Assignments for BITS

BITS Pin	Tip/Ring	CTC/TL1 Name	Function
A4	ring	BITS-1	Input from BITS device 1
B4	tip	BITS-1	Input from BITS device 1
A3	ring	BITS-1	Output to external device 1
B3	tip	BITS-1	Output to external device 1
A2	ring	BITS-2	Input from BITS device 2
B2	tip	BITS-2	Input from BITS device 2
A1	ring	BITS-2	Output to external device 2
B1	tip	BITS-2	Output to external device 2

Note For more detailed information about timing, refer to the *Cisco ONS 15454 Reference Manual*. To set up system timing, see the "NTP-A28 Set Up Timing" procedure on page 4-22.

Step 2 Return to your originating procedure (NTP).

DLP-A21 Install LAN Wires on the Backplane

Purpose	This task installs the LAN wires on the backplane.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2) wire, preferably CAT5 UTP
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Rather than using the LAN wires, you can use the LAN connection port on the TCC2 if preferred. Use either the backplane connection or the TCC2 front connection. You cannot use the LAN backplane pins and the LAN connection port on the TCC2 simultaneously; however, it is possible for you to make a direct connection from a computer to the LAN connection port on the TCC2 while the LAN backplane pins are in use as long as the computer that is connected directly to the TCC2 is not connected to a LAN.

Step 1 Using #22 or #24 AWG (0.51 mm^2 or 0.64 mm^2) wire or CAT5 UTP Ethernet cable, wrap the wires on the appropriate wire-wrap pins according to local site practice.

Caution Cross talk may result if both receive (Rx) and transmit (Tx) pins connect on the same twisted pair of wires from the CAT5 cable. The two Tx pins need to be on one twisted pair, and the two Rx pins need to be on another twisted pair.

A frame ground pin is located beneath each pin field (FG2 for the LAN pin field). Wrap the ground shield of the LAN interface cable to the frame ground pin. Table 1-3 shows the LAN pin assignments.

Table 1-3 LAN Pin Assignments

Pin Field	Backplane Pins	RJ-45 Pins	Function/Color
LAN 1 Connecting to data circuit-terminating equipment (DCE*) (a hub or switch); the ONS 15454 is a DCE	B2	1	TX+ white/green
	A2	2	TX- green
	B1	3	RX+ white/orange
	A1	6	RX- orange
LAN 1 Connecting to data terminal equipment (DTE) (a PC/workstation or router)	B1	1	RX+ white/green
	A1	2	RX- green
	B2	3	TX+ white/orange
	A2	6	TX- orange

Note The TCC2 does not support Ethernet polarity detection. If your Ethernet connection has incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), a “Lan Connection Polarity Reversed” condition is raised. This condition usually occurs during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire-wrap pins.

Step 2 Return to your originating procedure (NTP).

DLP-A22 Install the TL1 Craft Interface

Purpose	This task installs the TL1 craft interface using the craft backplane pins. You can also use a LAN cable connected to the TCC2 EIA/TIA-232 port to access a TL1 craft interface.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm² or 0.64 mm²) alarm wires
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Rather than using the craft pins, you can use a LAN cable connected to the TCC2 EIA/TIA-232 port to access a TL1 craft interface.

Step 1 Using #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire, wrap the craft interface wires on the appropriate wire-wrap pins according to local site practice.

Note For information about attaching ferrites to wire-wrap pin fields, see the “DLP-A31 Attach Ferrites to Wire-Wrap Pin Fields” task on page 1-64.

Step 2 Wrap the ground shield of the craft interface cable to the frame-ground pin.

Wrap the ground wire of your computer cable to pin A3 on the craft pin field. Table 1-4 shows the pin assignments for the CRAFT pin field.

Note You cannot use the craft backplane pins and the EIA/TIA-232 port on the TCC2 card simultaneously. Using a combination prevents access to the node or causes a loss in connectivity.

Table 1-4 Craft Interface Pin Assignments

Pin Field	Contact	Function
Craft	A1	Receive
	A2	Transmit
	A3	Ground
	A4	DTR

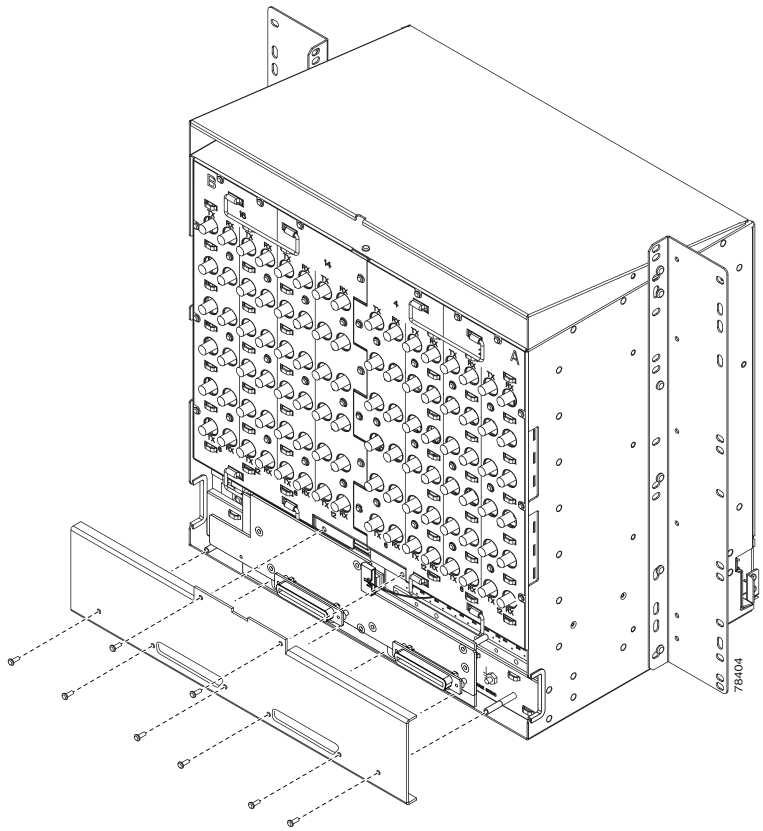
Step 3 Return to your originating procedure (NTP).

NTP-A120 Install an External Wire-Wrap Panel to the AEP

Purpose	This procedure connects an external wire-wrap panel to the AEP to provide the physical alarm contacts for the AEP.
Tools/Equipment	External wire-wrap panel
Prerequisite Procedures	NTP-A119 Install the Alarm Expansion Panel, page 1-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Position the lower cover over the AEP. Make sure that the AEP AMP Champ connectors protrude through the cutouts in the lower cover (Figure 1-18).

Figure 1-18 Installing the AEP Cover



Step 2 Insert and tighten the eight screws to secure the AEP cover to the AEP.

Step 3 Connect the cables from the external wire-wrap panel to the AMP Champ connectors on the AEP. Table 1-5 lists the alarm input pin assignments.

Table 1-5 Alarm Input Pin Assignments

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
1	ALARM_IN_1-	27	GND
2	GND	28	ALARM_IN_2-
3	ALARM_IN_3-	29	ALARM_IN_4-
4	ALARM_IN_5-	30	GND
5	GND	31	ALARM_IN_6-
6	ALARM_IN_7-	32	ALARM_IN_8-
7	ALARM_IN_9-	33	GND
8	GND	34	ALARM_IN_10-
9	ALARM_IN_11-	35	ALARM_IN_12-
10	ALARM_IN_13-	36	GND
11	GND	37	ALARM_IN_14-
12	ALARM_IN_15-	38	ALARM_IN_16-

Table 1-5 Alarm Input Pin Assignments (continued)

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
13	ALARM_IN_17-	39	GND
14	GND	40	ALARM_IN_18-
15	ALARM_IN_19-	41	ALARM_IN_20-
16	ALARM_IN_21-	42	GND
17	GND	43	ALARM_IN_22-
18	ALARM_IN_23-	44	ALARM_IN_24-
19	ALARM_IN_25-	45	GND
20	GND	46	ALARM_IN_26-
21	ALARM_IN_27-	47	ALARM_IN_28-
22	ALARM_IN_29-	48	GND
23	GND	49	ALARM_IN_30-
24	ALARM_IN_31-	50	—
25	ALARM_IN_+	51	GND1
26	ALARM_IN_0-	52	GND2

Table 1-6 lists the alarm output pin assignments.

Table 1-6 Alarm Output Pin Assignments

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
1	—	27	COM_0
2	COM_1	28	—
3	NO_1	29	NO_2
4	—	30	COM_2
5	COM_3	31	—
6	NO_3	32	NO_4
7	—	33	COM_4
8	COM_5	34	—
9	NO_5	35	NO_6
10	—	36	COM_6
11	COM_7	37	—
12	NO_7	38	NO_8
13	—	39	COM_8
14	COM_9	40	—
15	NO_9	41	NO_10
16	—	42	COM_10
17	COM_11	43	—

Table 1-6 Alarm Output Pin Assignments (continued)

AMP Champ Pin	Signal Name	AMP Champ Pin	Signal Name
18	NO_11	44	NO_12
19	—	45	COM_12
20	COM_13	46	—
21	NO_13	47	NO_14
22	—	48	COM_14
23	COM_15	49	—
24	NO_15	50	—
25	—	51	GND1
26	NO_0	52	GND2

Figure 1-19 illustrates the alarm input connectors.

Figure 1-19 Alarm Input Connector

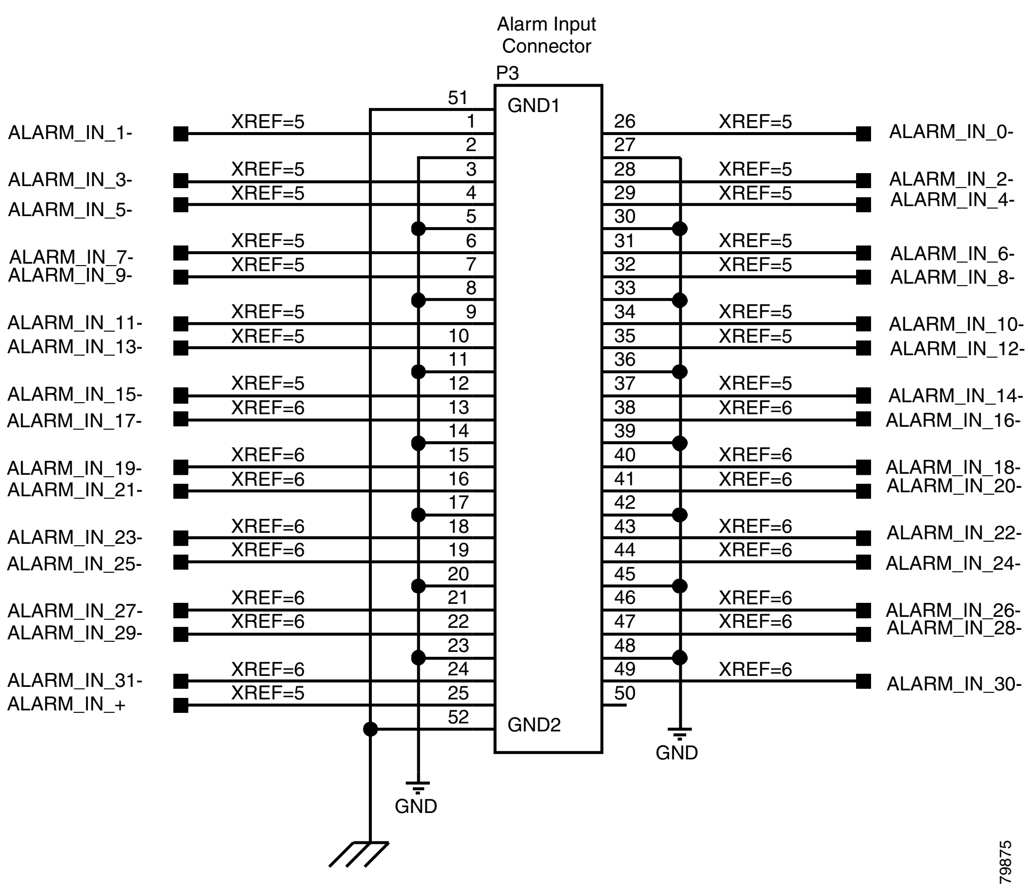
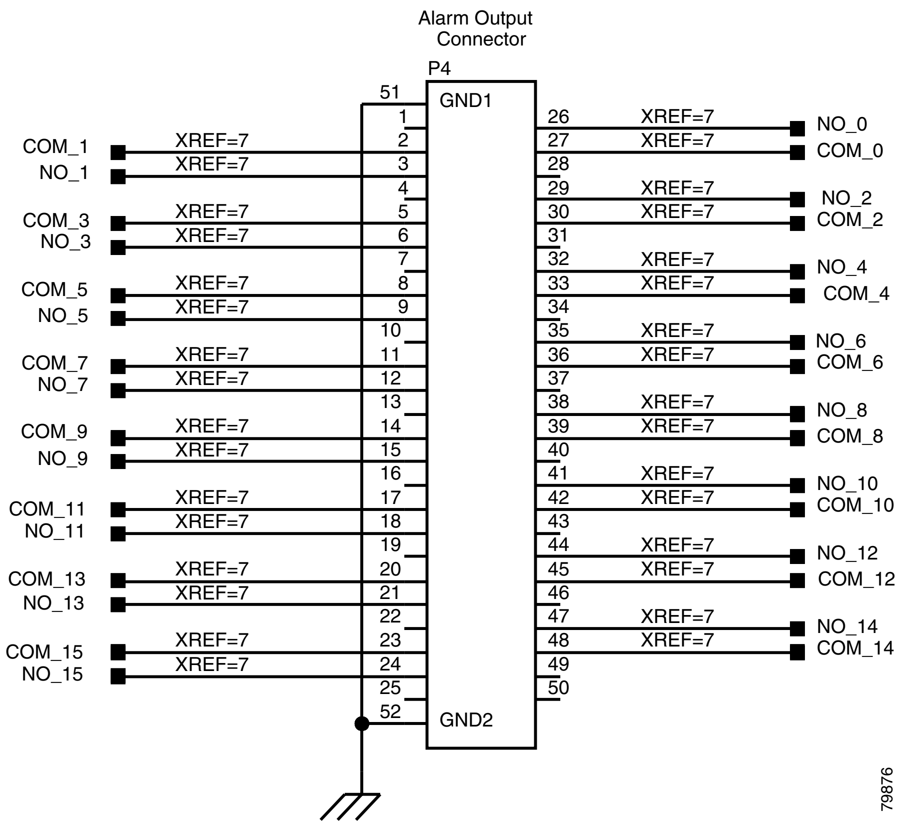


Figure 1-20 illustrates the alarm output connectors.

Figure 1-20 Alarm Output Connector



Step 4 Complete one of the following:

- If you plan to install electrical cards, continue with the "NTP-A9 Install the Electrical Card Cables on the Backplane" procedure on page 1-49.
- If you do not plan to install electrical cards, continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-60.

Stop. You have completed this procedure.

NTP-A9 Install the Electrical Card Cables on the Backplane

Purpose	Optional electrical interface assembly (EIA) backplane covers are typically pre-installed when ordered with the ONS 15454. The following procedure describes how to install the electrical card cables to the backplane. If the shelf was not shipped with the correct EIA interface, you must order and install the correct EIA.
Tools/Equipment	Wire wrapper Twisted-pair cables BNC insertion tool SMB cable connector #2 Phillips screwdriver Medium slot-head screwdriver DS-1 and DS-3 cables, as needed Tie-down bar, as needed
Prerequisite Procedures	NTP-A5 Install the EIAs, page 1-17
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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 Refer to the *Cisco ONS 15454 Reference Manual* for more information about EIAs.

Step 1 Complete the "DLP-A530 Install the Tie-Down Bar" task on page 1-50 as needed for routing the electrical cables you will install.

Step 2 Complete the "DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)" task on page 1-51 as needed. Baluns are used on SMB EIAs to properly terminate DS-1 signals.

Step 3 To install DS-1 cables using AMP Champ cables, complete the "DLP-A24 Install DS-1 AMP Champ Cables on the AMP Champ EIA" task on page 1-52.

Step 4 Complete the "DLP-A25 Install Coaxial Cable With BNC Connectors" task on page 1-55 as needed.

Step 5 Complete the "DLP-A26 Install Coaxial Cable With High-Density BNC Connectors" task on page 1-56 as needed.

Step 6 Complete the "DLP-A27 Install Coaxial Cable with SMB Connectors" task on page 1-57 as needed.

Step 7 Continue with the "NTP-A10 Route Electrical Cables" procedure on page 1-58.

Stop. You have completed this procedure.

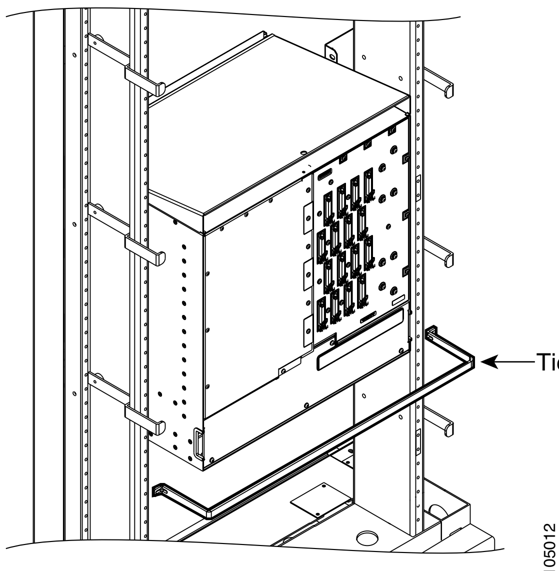
DLP-A530 Install the Tie-Down Bar

Purpose	This task installs the tie-down bar used to secure cabling on the rear of the ONS 15454. The tie-down bar can be used to provide a diverse path for redundant power feeds and cables.
Tools/Equipment	Tie-down bar Screws (4)
Prerequisite Procedures	DLP-A5 Mount the Shelf Assembly in a Rack (One Person), page 1-10 DLP-A6 Mount the Shelf Assembly in a Rack (Two People), page 1-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the ends of the tie-down bar with the four screw holes located 1 RU below the ONS 15454.

Figure 1-21 shows the tie-down bar, the ONS 15454, and the rack.

Figure 1-21 Tie-Down Bar



Step 2 Install the four screws into the rack.

Step 3 Return to your originating procedure (NTP).

DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)

Purpose	This task installs the DS-1 cables on an SMB EIA using the electrical interface adapters.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 1-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note All DS-1 cables connected to the ONS 15454 DS-1 ports must terminate with twisted-pair cables to connect to the DS-1 electrical interface adapter. The DS-1 electrical interface adapters project 1.72 inches (43.7 mm) beyond the SMB EIA. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Attach the SMB connector on an adapter to the SMB connector for the port's transmit pair on the backplane.

Step 2 Attach the SMB connector on an adapter to the SMB connector for the port's receive pair on the backplane.

Step 3 Terminate the DS-1 transmit and receive cables for the port to the wire-wrap posts on the adapter:

a. Using a wire-wrap tool, connect the receive cables to the receive adapter pins on the backplane connector for the desired port.

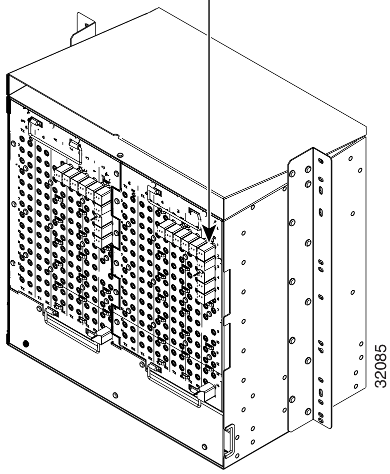
b. Connect the transmit cables to the transmit adapter pins on the backplane connector for the desired port.

c. Terminate the shield ground wire on the DS-1 cable to ground according to local site practice.

Note If you put DS1N-14 cards in Slots 3 and 15 to form 1:N protection groups, do not wire Slots 3 and 15 for DS-1 electrical interface adapters.

Figure 1-22 shows a ONS 15454 backplane with an SMB EIA. DS-1 electrical interface adapters are attached on both sides of the shelf assembly to create DS-1 twisted-pair termination points.

Figure 1-22 Backplane with an SMB EIA for DS-1 Cables



Step 4 Return to your originating procedure (NTP).

DLP-A24 Install DS-1 AMP Champ Cables on the AMP Champ EIA

Purpose	This task installs the DS-1 AMP Champ cables on the AMP Champ EIA.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A14 Install the AMP Champ EIA, page 1-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Prepare a 56-wire cable for each DS1-14/DS1N-14 card you will install in the shelf assembly.

Step 2 Connect the male AMP Champ connector on the cable to the female AMP Champ connector on the ONS 15454 backplane.

Step 3 Use the clips on the male AMP Champ connector to secure the connection.

The female connector has grooves on the outside edge for snapping the clips into place.

Table 1-7 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA.

Note In Table 1-7, the shaded area corresponds to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 1-7 Pin Assignments for AMP Champ Connectors

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 [1] white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare0+ Not applicable	15	47	Tx Spare0- Not applicable	Rx Spare0+ Not applicable	31	63	Rx Spare0- Not applicable
Tx Spare1+ Not applicable	16	48	Tx Spare1- Not applicable	Rx Spare1+ Not applicable	32	64	Rx Spare1- Not applicable

1. Shaded areas correspond to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 1-8 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA for a shielded DS-1 cable.

Table 1-8 Pin Assignments for AMP Champ Connectors (Shielded DS1 Cable)

64-Pin Blue Bundle				64-Pin Orange Bundle			
Signal/Wire	**Pin**	**Pin**	**Signal/Wire**	**Signal/Wire**	**Pin**	**Pin**	**Signal/Wire**
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 white/blue	17	49	Rx Ring 1 blue/white
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 white/orange	18	50	Rx Ring 2 orange/white
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 white/green	19	51	Rx Ring 3 green/white
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 white/brown	20	52	Rx Ring 4 brown/white
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 white/slate	21	53	Rx Ring 5 slate/white
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 red/blue	22	54	Rx Ring 6 blue/red
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 red/orange	23	55	Rx Ring 7 orange/red
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 red/green	24	56	Rx Ring 8 green/red
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 red/brown	25	57	Rx Ring 9 brown/red
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 red/slate	26	58	Rx Ring 10 slate/red
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 black/blue	27	59	Rx Ring 11 blue/black
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 black/orange	28	60	Rx Ring 12 orange/black
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 black/green	29	61	Rx Ring 13 green/black
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 black/brown	30	62	Rx Ring 14 brown/black
Tx Tip 15 black/slate	15	47	Tx Tip 15 slate/black	Rx Tip 15 black/slate	31	63	Rx Tip 15 slate/black
Tx Tip 16 yellow/blue	16	48	Tx Tip 16 blue/yellow	Rx Tip 16 yellow/blue	32	64	Rx Tip 16 blue/yellow

Step 4 Return to your originating procedure (NTP).

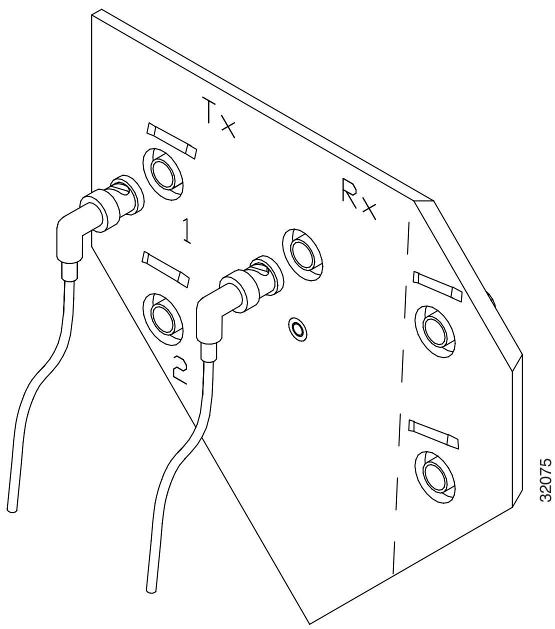
DLP-A25 Install Coaxial Cable With BNC Connectors

Purpose	This task installs the coaxial cable with BNC connectors.
Tools/Equipment	None
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 1-19
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Place the BNC cable connector over the desired connection point on the backplane.

Figure 1-23 shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

Figure 1-23 Using a Right-Angle Connector to Install Coaxial Cable with BNC Connectors



Step 2 Position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector clockwise to lock it into place.

Step 5 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice. The rubber-coated edges of the side cutouts prevent the cables from chafing.

Warning **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3, etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.**

Step 7 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 8 Return to your originating procedure (NTP).

DLP-A26 Install Coaxial Cable With High-Density BNC Connectors

Purpose	This task installs the coaxial cable with high-density BNC connectors.
Tools/Equipment	BNC insertion tool
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 1-19
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Place the cable connector over the desired connection point on the backplane.

Step 2 Using the BNC insertion tool, position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector clockwise to lock it into place.

Step 5 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.

Warning **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3, etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.**

The rubber-coated edges of the side cutouts prevent the cables from chafing.

Step 7 Return to your originating procedure (NTP).

DLP-A27 Install Coaxial Cable with SMB Connectors

Purpose	This task installs the coaxial cable with SMB connectors.
Tools/Equipment	SMB cable connector
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 1-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

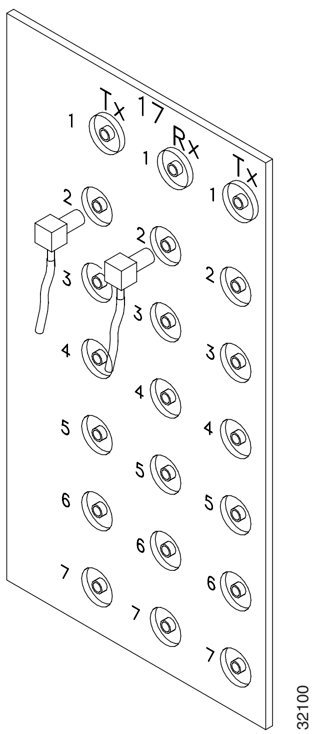
Step 1 Place the SMB cable connector over the desired connection point on the backplane (Figure 1-24).

Step 2 Gently push the connector until it clicks into place.

Step 3 Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

Step 4 Route the cables to the nearest side of the shelf assembly into rack runs according to local site practice.

Figure 1-24 Installing Coaxial Cable with SMB Connectors



Warning **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3, etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.**

Step 5 Label the transmit, receive, working, and protect cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 6 Return to your originating procedure (NTP).

NTP-A10 Route Electrical Cables

Purpose	This procedure routes and manages electrical (backplane) cables.
Tools/Equipment	RG179, RG59 (735A) # 26 AWG cable, or RG59 (734A) # 20 AWG cable
Prerequisite Procedures	NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-49
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A28 Route Coaxial Cables" task on page 1-58 as needed.

Step 2 Complete the "DLP-A29 Route DS-1 Twisted-Pair Cables" task on page 1-60 as needed.

Step 3 Continue with the "NTP-A11 Install the Rear Cover" procedure on page 1-60.

Stop. You have completed this procedure.

DLP-A28 Route Coaxial Cables

Purpose	This task routes the coaxial cables.
Tools/Equipment	RG179, RG59 (735A) # 26 AWG cable, or RG59 (734A) # 20 AWG cable
Prerequisite Procedures	One or more of the following tasks, as needed: • DLP-A25 Install Coaxial Cable With BNC Connectors, page 1-55 • DLP-A26 Install Coaxial Cable With High-Density BNC Connectors, page 1-56 • DLP-A27 Install Coaxial Cable with SMB Connectors, page 1-57
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Tie wrap or lace the coaxial cables according to local site practice and route the cables through the side cutouts on either side of the ONS 15454. The rubber coated edges of the side cutouts prevent the cables from chafing.

Step 2 Use short lengths of pigtail RG179 to terminate the shelf assembly.

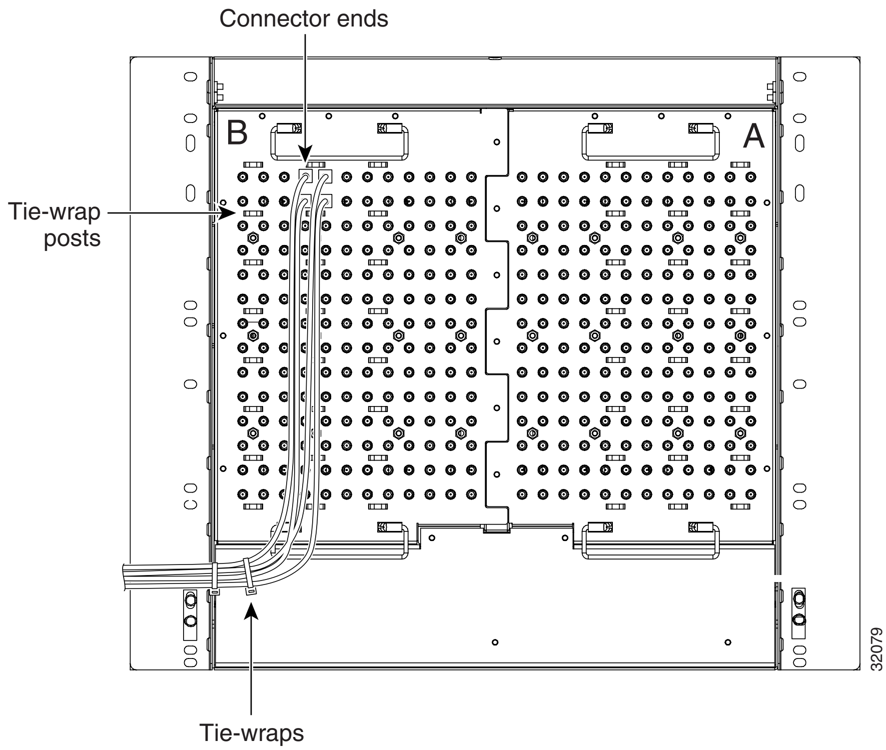
Step 3 Use standard RG59 (735A) cable connected to the RG179 for the remainder of the cable run. When using a 10-foot (3.05 m) section of the RG179, you can attach a maximum length of 437 feet (133 m) of RG59 (735A). When using a 30-foot (9.1 m) section of RG179, you can attach a maximum length of 311 feet (94.8 m) of RG59 (735A).

When using the RG179 cable, the maximum distance available (122 feet, 37.2 m) is less than the maximum distance available with standard RG59 (735A) cable (306 feet, 93.3 m). The maximum distance when using the RG59 (734A) cable is 450 feet (137.2 m). The shorter maximum distance available with the RG179 is due to a higher attenuation rate for the thinner cable. Attenuation rates are calculated using a DS-3 signal:

- For RG179, the attenuation rate is 59 dB/kft (dB per kilo-foot) at 22 MHz.
- For RG59 (735A), the attenuation rate is 23 dB/kft at 22 MHz.

Use a figure of 5.0 for total cable loss when making calculations. Figure 1-25 shows an example of proper coaxial cable routing.

Figure 1-25 Routing Coaxial Cable (SMB EIA Backplane)



Step 4 Return to your originating procedure (NTP).

DLP-A29 Route DS-1 Twisted-Pair Cables

Purpose	This task routes the DS-1 twisted-pair cables.
Tools/Equipment	None
Prerequisite Procedures	DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun), page 1-51
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the following:

- DS-1 electrical interface adapters are installed on every transmit and receive connector for DS-1 ports.
- Wire-wrap posts on the DS-1 electrical interface adapters are used to connect the terminated incoming cables.

Step 2 Tie-wrap or lace the twisted-pair cables according to local site practice and route the cables into the side cutouts on either side of the ONS 15454.

Note SMB EIAs feature cable-management eyelets for tie wrapping or lacing cables to the cover panel.

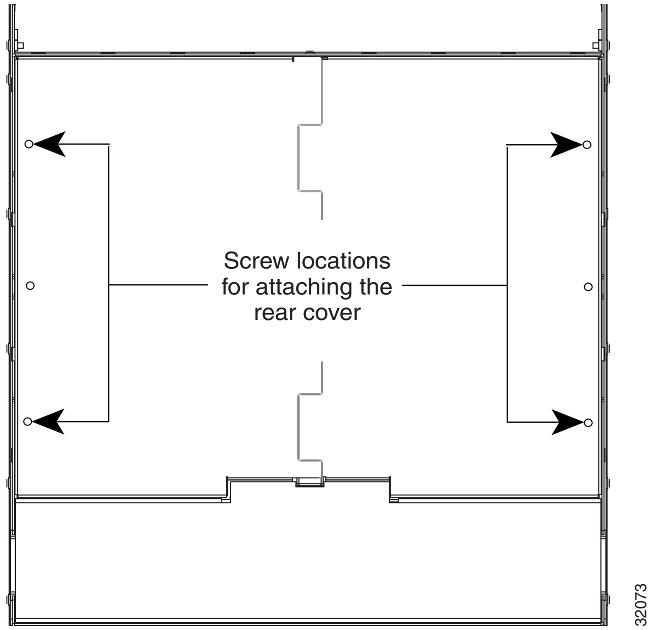
Step 3 Return to your originating procedure (NTP).

NTP-A11 Install the Rear Cover

Purpose	The following procedure explains how to install the rear cover.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Locate the three screws that run vertically along both edges of the backplane (Figure 1-26).

Figure 1-26 Backplane Attachment for the Rear Cover



Tip Only six screws (three on each side) line up with the screw slots on the mounting brackets, making the screws easy to locate.

Step 2 Loosen the top and bottom screws on one edge of the backplane to provide room to slide the mounting brackets into place using the u-shaped screw slots on each end.

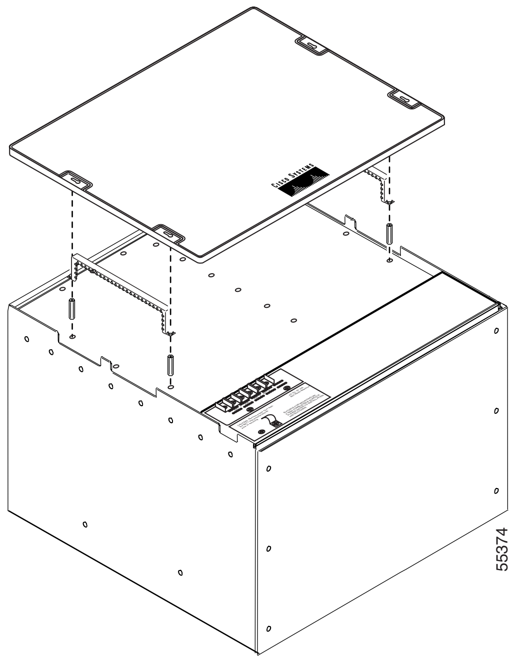
Step 3 Slide one of the mounting brackets into place and tighten the screws.

Step 4 Repeat Steps 2 and 3 for the second mounting bracket.

Step 5 Attach the cover by hanging it from the mounting screws on the back of the mounting brackets and pulling it down until it fits snugly into place.

Figure 1-27 shows rear cover installation using spacers.

Figure 1-27 Installing the Rear Cover with Spacers



Step 6 Continue with the "NTP-A12 Install Ferrites" procedure on page 1-62.

Stop. You have completed this procedure.

NTP-A12 Install Ferrites

Purpose	This procedure describes how to attach ferrites.
Tools/Equipment	Oval and block ferrites
Prerequisite Procedures	NTP-A6 Install the Power and Ground, page 1-25
	NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-37
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A30 Install Ferrites to Power Cabling" task on page 1-63 as needed.

Step 2 Complete the "DLP-A31 Attach Ferrites to Wire-Wrap Pin Fields" task on page 1-64 as needed.

Step 3 Continue with the "NTP-A13 Perform the Shelf Installation Acceptance Test" procedure on page 1-67.

Stop. You have completed this procedure.

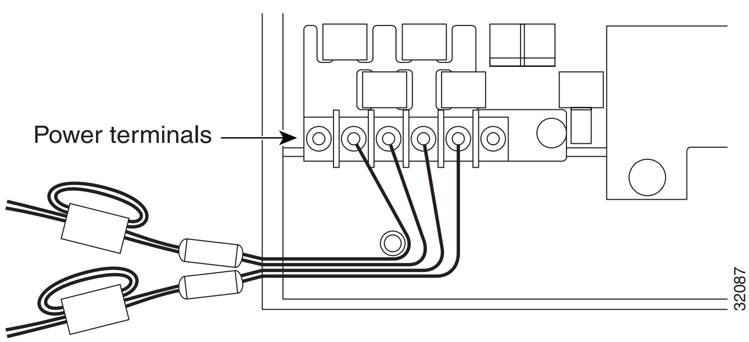
DLP-A30 Install Ferrites to Power Cabling

Purpose	This task attaches ferrites to power cabling. Use a single oval ferrite (TDK ZCAT2035-0930) and a single block ferrite (Fair Rite 0443164151) for each pair of cables (BAT1/RET1 [A] and BAT2/RET2[B]).
Tools/Equipment	Oval and block ferrites
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Wrap the cables once around and through the block ferrites and pull the cables straight through the oval ferrites.

Step 2 Place the oval ferrite as close to the power terminals as possible, between the ONS 15454 and the block ferrite, as shown in Figure 1-28. The block ferrite should be within 5 to 6 inches (127 to 152 mm) of the power terminals.

Figure 1-28 Attaching Block and Oval Ferrites to Power Cabling



Step 3 Return to your originating procedure (NTP).

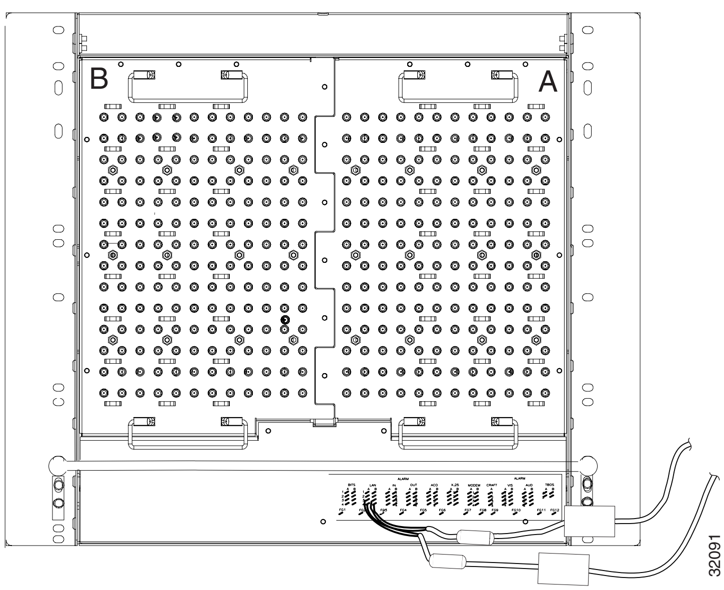
DLP-A31 Attach Ferrites to Wire-Wrap Pin Fields

Purpose	This task attaches ferrites to wire-wrap pin fields. Use an oval ferrite (TDK ZCAT1730-0730) and block ferrite (Fair Rite 0443164151) for each pair of cables. Figure 1-29 on page 1-64 shows the suggested method for attaching ferrites to wire-wrap pin fields.
Tools/Equipment	Oval and block ferrites
Prerequisite Procedures	NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-37
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Wrap the cables once around and through the block ferrites and pull the cables straight through the oval ferrites.

Step 2 Place the oval ferrite as close to the wire-wrap pin field as possible and between the ONS 15454 and the block ferrite, as shown in Figure 1-29. The block ferrite should be within 5 to 6 inches (127 to 152 mm) of the wire-wrap pin field.

Figure 1-29 Attaching Ferrites to Wire-Wrap Pin Fields



Step 3 Return to your originating procedure (NTP).

NTP-A238 Install Optional DWDM Equipment

Purpose	This procedure installs the optional DWDM assemblies.
Tools/Equipment	# 2 Phillips screwdriver Crimping tool (large enough for #10 - #14 AWG) #14 AWG wire
Prerequisite Procedures	NTP-A2 Install the Shelf Assembly, page 1-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-A412 Install the DCU Shelf Assembly" task on page 1-65 as needed.

Step 2 Complete the "DLP-A413 Install the Fiber Patch Panel Shelf" task on page 1-66 as needed.

Step 3 Complete the "DLP-A414 Install the Fiber Storage Shelf" task on page 1-66 as needed.

Step 4 Complete the "DLP-A415 Install the Air Ramp" task on page 1-67 as needed.

Stop. **You have completed this procedure**.

DLP-A412 Install the DCU Shelf Assembly

Purpose	If you are installing dispersion compensation modules, use this task to install the dispersion compensation unit (DCU) chassis.
Tools/Equipment	#2 Phillips screwdriver Crimping Tool #14 AWG wire and lug
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 The DCU chassis requires 1-RU in a standard 19-inch or 23-inch rack. Locate the RMU space specified in your site plan. Refer to *Cisco ONS 15454 Reference Manual* for typical DWDM site layout plans.

Step 2 Two sets of mounting brackets are included with the DCU mounting kit, one set each, for 19-inch or 23-inch racks. Verify that your chassis is equipped with the correct set of brackets for your rack. Change the brackets as required.

Step 3 Align the chassis with the rack mounting screw holes; one at a time insert and tighten the four screws.

Warning **This equipment must be properly grounded per local standards and in compliance with NEBS. If not properly grounded-personal injury or equipment failure could occur.**

Step 4 Connect a frame ground to the ground terminal provided on either side of the chassis. Use minimum #14 AWG wire.

Step 5 Return to your originating procedure (NTP).

DLP-A413 Install the Fiber Patch Panel Shelf

Purpose	This task installs the fiber patch panel shelf.
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 The Fiber Patch Panel shelf requires 1-RU in a standard 19-inch or 23-inch rack. Locate the RMU space specified in your site plan. Refer to *Cisco ONS 15454 Reference Manual* for typical DWDM site layout plans.

Step 2 Verify that the mounting brackets attached to the unit are correct for your rack size. Complete "DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack" task on page 1-7 as required.

Step 3 Align the chassis with the rack mounting screw holes, then insert and tighten the four screws.

Step 4 Return to your originating procedure (NTP).

DLP-A414 Install the Fiber Storage Shelf

Purpose	This task installs the fiber storage shelf.
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 The fiber storage shelf requires 1-RU in a standard 19-inch or 23-inch rack. Locate the RMU space specified in your site plan. Refer to *Cisco ONS 15454 Reference Manual* for typical DWDM site layout plans.

Step 2 Verify that the mounting brackets attached to the unit are correct for your rack size. Complete "DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack" task on page 1-7 as required.

Step 3 Align the chassis with the rack mounting screw holes, insert the screws (4) and tighten.

Step 4 Return to your originating procedure (NTP).

DLP-A415 Install the Air Ramp

Purpose	Use this task to install the air ramp.
Tools/Equipment	#2 Phillips screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 The air ramp requires 1-RU in a standard 19-inch or 23-inch rack. Locate the RMU space specified in your site plan. Refer to *Cisco ONS 15454 Reference Manual* for typical DWDM site layout plans.

Step 2 Verify that the mounting brackets attached to the unit are correct for your rack size. Complete "DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack" task on page 1-7 as required.

Step 3 Align the chassis with the rack mounting screw holes; insert and tighten the four screws.

Step 4 Return to your originating procedure (NTP).

NTP-A13 Perform the Shelf Installation Acceptance Test

Purpose	Use this procedure to perform a shelf installation acceptance test.
Tools/Equipment	Voltmeter, oval and block ferrites
Prerequisite Procedures	Applicable procedures in Chapter 1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete Table 1-9 by verifying that each applicable procedure was completed.

Table 1-9 Shelf Installation Task Summary

Description	Completed
NTP-A1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4	
NTP-A2 Install the Shelf Assembly, page 1-6	
NTP-A3 Open and Remove the Front Door, page 1-13	
NTP-A4 Remove the Backplane Covers, page 1-16	
NTP-A5 Install the EIAs, page 1-17	
NTP-A6 Install the Power and Ground, page 1-25	
NTP-A7 Install the Fan-Tray Assembly, page 1-31	
NTP-A119 Install the Alarm Expansion Panel, page 1-34	
NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-37	

Table 1-9 Shelf Installation Task Summary (continued)

Description	Completed
NTP-A120 Install an External Wire-Wrap Panel to the AEP, page 1-44	
NTP-A9 Install the Electrical Card Cables on the Backplane, page 1-49	
NTP-A10 Route Electrical Cables, page 1-58	
NTP-A11 Install the Rear Cover, page 1-60	
NTP-A238 Install Optional DWDM Equipment, page 1-65	

Step 2 Complete the "DLP-A32 Inspect the Shelf Installation and Connections" task on page 1-68.

Step 3 Complete the "DLP-A33 Measure Voltage" task on page 1-68.

Step 4 Continue with Chapter 2, "Install Cards and Fiber-Optic Cable."

Stop. You have completed this procedure.

DLP-A32 Inspect the Shelf Installation and Connections

Purpose	Use this task to inspect the shelf installation and connections and to verify that everything is installed and connected properly.
Tools/Equipment	None
Prerequisite Procedures	Complete Table 1-9 on page 1-67
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 2 To check that the backplane is seated correctly, verify that the screw holes and the backplane interface card holes align properly and that the A and B connectors interlock.

Step 3 Return to your originating procedure (NTP).

DLP-A33 Measure Voltage

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Complete Table 1-9 on page 1-67.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office ground and power. Figure 1-10 on page 1-29 shows the power terminals.

a. Place the black lead (positive) on the frame ground on the bay. Hold it there while completing Step b.

b. Place the red lead (negative) on the fuse power points and alarm panel to verify that they read between –40.5 VDC and –57 VDC (power) or 0 (return ground).

Step 2 Using a voltmeter, verify the shelf ground and power wiring:

a. Place the black lead (positive) on the RET1 and the red lead on the BAT1 point. Verify a reading between –40.5 VDC and –57 VDC. If there is no voltage, check the following and correct if necessary:

- Battery and ground are reversed to the shelf.
- Battery is open or missing.
- Return is open or missing.

b. Repeat Step 2 for the RET2 and BAT2 if the B power feed is provided

Step 3 Return to your originating procedure (NTP).

Install Cards and Fiber-Optic Cable

This chapter explains how to install the Cisco ONS 15454 cards and fiber-optic cable (fiber).

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A15 Install the Common Control Cards, page 2-2—Complete this procedure first before installing any other cards.
2. NTP-A16 Install the OC-N Cards, page 2-12—Complete as needed.
3. NTP-A249 Install the Transponder and Muxponder Cards, page 2-14—Complete as needed.
4. NTP-A17 Install the Electrical Cards, page 2-16—Complete as needed.
5. NTP-A246 Install Ethernet Cards and Connectors, page 2-17—Complete as needed.
6. NTP-A274 Install the FC_MR-4 Cards, page 2-23—Complete as needed.
7. NTP-A247 Install Fiber-Optic Cables on OC-N Cards, page 2-29—Complete this procedure to install fiber on OC-N cards, Ethernet Gigabit Interface Converters (GBICs), or small form-factor pluggables (SFPs).
8. NTP-A242 Install the DWDM Cards, page 2-25—Complete as needed.
9. NTP-A243 Install the DWDM Dispersion Compensating Cards, page 2-28—Complete as needed.
10. NTP-A244 Install Fiber-Optic Cables on DWDM Cards, page 2-41—Complete as needed.
11. NTP-A245 Route Fiber-Optic Cables, page 2-56—Complete as needed.
12. NTP-A116 Remove and Replace a Card, page 2-57—Complete this procedure as needed to remove and replace a card, including deleting the card from Cisco Transport Controller (CTC) and changing an OC-N card without losing the card's provisioning.
13. NTP-A20 Replace the Front Door, page 2-59—If the front door was removed, complete this procedure to replace the front door and ground strap after installing cards and fiber.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Caution Unused card slots should be filled with a blank faceplate (Cisco P/N 15454-BLANK). The blank faceplate ensures proper airflow when operating the ONS 15454 without the front door attached, although Cisco recommends that the front door remain attached.

NTP-A15 Install the Common Control Cards

Purpose	This procedure describes how to install the common control cards.
Tools/Equipment	Redundant TCC2 cards
	Redundant XC, XCVT, or XC10G (cross-connect) cards
	AIC/AIC-I card (optional)
Prerequisite Procedures	NTP-A13 Perform the Shelf Installation Acceptance Test, page 1-67
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Step 1 If you plan to install XC/XCVT cards, review Table 2-1 to determine card/slot compatibility. If you plan to install XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Complete the "DLP-A36 Install the TCC2 Cards" task on page 2-7.

Step 3 Complete the "DLP-A37 Install the XC, XCVT, or XC10G Cards" task on page 2-9 unless you are provisioning a DWDM-only node.

Step 4 Complete the "DLP-A38 Install the Alarm Interface Controller or Alarm Interface Controller–International Card" task on page 2-11, as needed.

Note If you install the wrong card in a slot, see the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 5 Continue with one of the following:

- If the node you are provisioning is TDM-only (no DWDM cards installed), install the traffic cards. To determine the appropriate procedure, see the NTP list in the "Before You Begin" section on page 2-1.
- If the node you are provisioning is DWDM-only or a hybrid, continue with Chapter 3, "Connect the PC and Log into the GUI."

In Table 2-1, X indicates that a card is supported in the slot.

Table 2-1 Card and Slot Compatibility for the XC and XCVT Cards

Slot	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Type	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**	**HS[2]**	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**
TCC2							X				X						
XC/XCVT								X		X							
AIC									X								
AIC-I									X								
DS1-14	X	X	X	X	X	X						X	X	X	X	X	X
DS1N-14	X[3]	X[3]	X	X[3]	X[3]	X[3]						X[3]	X[3]	X[3]	X	X[3]	X[3]
DS3-12	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
DS3-12E	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
DS3N-12	X[3]	X[3]	X	X[3]	X[3]	X[3,4]						X[3,4]	X[3]	X[3]	X	X[3]	X[3]
DS3N-12E	X[3]	X[3]	X	X[3]	X[3]	X[3,4]						X[3,4]	X[3]	X[3]	X	X[3]	X[3]
DS3I-N-12[5]	X[3]	X[3]	X	X[3]	X[3]	X[3,]						X[3,]	X[3]	X[3]	X	X[3]	X[3]
DS3XM-6	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
EC1-12	X	X	X	X	X	X[6]						X[6]	X	X	X	X	X
E100T-12	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2	X	X	X	X	X	X						X	X	X	X	X	X
E100T-G	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2-G	X	X	X	X	X	X						X	X	X	X	X	X
G1000-4	Not supported with XC/XCVT cards. Requires XC10G cards.																
G1K-4					X	X						X	X				
ML100-12					X	X						X	X				
ML1000-2					X	X						X	X				
OC3 IR 4/STM1 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC3IR/STM1SH 1310-8	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC12 IR STM4 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 LR/STM4 LH 1310	X	X	X	X	X	X						X	X	X	X	X	X

Table 2-1 Card and Slot Compatibility for the XC and XCVT Cards (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**[1]	**MS**[1]	**MS**[1]	**MS**[1]	**HS**[2]	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS**[1]	**MS**[1]	**MS**[1]	**MS**[1]
OC12 LR/STM4 LH 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC12 IR/STM4 SH 1310-4	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC48 IR 1310[7]					X	X						X	X				
OC48 LR 1550					X	X						X	X				
OC48 IR/STM16 SH AS 1310					X	X						X	X				
OC48 LR/STM16 LH AS 1550					X	X						X	X				
OC48-ELR/STM 16 EH 100 GHz					X	X						X	X				
OC48 ELR 200 GHz					X	X						X	X				
OC192 SR/STM64 IO 1310	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC192 IR/STM64 SH 1550	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC192 LR/STM64 LH 1550	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC192 LR/STM64 LH ITU 15xx.xx	Not supported with XC/XCVT cards. Requires XC10G cards.																
TXP_MR_2.5G	X	X	X	X	X	X						X	X	X	X	X	X
TXPP_MR_2.5G	X	X	X	X	X	X						X	X	X	X	X	X
TXP_MR_10G	X	X	X	X	X	X						X	X	X	X	X	X
FC_MR-4					X	X						X	X				
MXP_2.5G_10G	X	X	X	X	X	X						X	X	X	X	X	X

1. MS identifies slots 1 to 4 and 14 to 17 (“multispeed” slot).
2. HS identifies slots 5, 6, 12, and 13 (“high-speed” slot).
3. This identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.
4. This DS3 card cannot be used in this slot if used with a high-density EIA or in a 1:N configuration.
5. This card can only be use with the XCVT card, not the XC card.
6. EC1 cards cannot be used in this slot if used with a high-density EIA.
7. The OC48AS will operate in the high speed slots with the XC/XCVT in R3.4 and later. In Release R3.3, OC48AS with XC/XCVT is not supported.

In Table 2-2, X indicates that a card is supported in the slot. The XC10G card requires the ANSI shelf (5454-SA-ANSI) or the high-density shelf (15454-SA-HD).

Table 2-2 Card and Slot Compatibility for the XC10G Card

Slot	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Type	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**	**HS[2]**	**HS[2]**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS[2]**	**HS[2]**	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**
TCC2							X				X						
XC10G								X		X							
AIC									X								
AIC-I									X								
DS1-14	X	X	X	X	X	X						X	X	X	X	X	X
DS1N-14	X[3]	X[3]	X	X[3]	X[3]	X[3]						X[3]	X[3]	X[3]	X	X[3]	X[3]
DS3-12	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
DS3-12E	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
DS3N-12	X[3]	X[3]	X	X[3]	X[3]	X[3,4]						X[3,4]	X[3]	X[3]	X	X[3]	X[3]
DS3N-12E	X[3]	X[3]	X	X[3]	X[3]	X[3,4]						X[3,4]	X[3]	X[3]	X	X[3]	X[3]
DS3XM-6	X	X	X	X	X	X[4]						X[4]	X	X	X	X	X
EC1-12	X	X	X	X	X	X[5]						X[5]	X	X	X	X	X
E100T-12	Not supported with the XC10G card.																
E1000-2	Not supported with the XC10G card.																
E100T-G	X	X	X	X	X	X						X	X	X	X	X	X
E1000-2-G	X	X	X	X	X	X						X	X	X	X	X	X
G1000-4	X	X	X	X	X	X						X	X	X	X	X	X
G1K-4	X	X	X	X	X	X						X	X	X	X	X	X
ML100-12	X	X	X	X	X	X						X	X	X	X	X	X
ML1000-2	X	X	X	X	X	X						X	X	X	X	X	X
OC3 IR 4/STM1 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC3IR/STM1SH 1310-8	X	X	X	X										X	X	X	X
OC12 IR STM4 SH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 LR/STM4 LH 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC12 IR/STM4 SH 1310-4	X	X	X	X										X	X	X	X
OC12 LR/STM4 LH 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC48 IR 1310					X	X						X	X				
OC48 LR 1550					X	X						X	X				

Table 2-2 Card and Slot Compatibility for the XC10G Card (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**	**HS[2]**	**HS[2]**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS[2]**	**HS[2]**	**MS[1]**	**MS[1]**	**MS[1]**	**MS[1]**
OC48 IR/STM16 SH AS 1310	X	X	X	X	X	X						X	X	X	X	X	X
OC48 LR/STM16 LH AS 1550	X	X	X	X	X	X						X	X	X	X	X	X
OC48-ELR/STM16 EH 100 GHz					X	X						X	X				
OC48 ELR 200 GHz					X	X						X	X				
OC192 SR/STM64 IO 1310					X	X						X	X				
OC192 IR/STM64 SH 1550					X	X						X	X				
OC192 LR/STM64 LH 1550					X	X						X	X				
OC192 LR/STM64 LH ITU 15xx.xx					X	X						X	X				
TXP_MR_2.5G	X	X	X	X	X	X						X	X	X	X	X	X
TXPP_MR_2.5G	X	X	X	X	X	X						X	X	X	X	X	X
TXP_MR_10G	X	X	X	X	X	X						X	X	X	X	X	X
MXP_2.5G_10G	X	X	X	X	X	X						X	X	X	X	X	X
FC_MR-4	X	X	X	X	X	X						X	X	X	X	X	X

1. MS identifies slots 1 to 4 and 14 to 17 (“multispeed” slot).
2. HS identifies slots 5, 6, 12, and 13 (“high-speed” slot).
3. This identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.
4. This DS3 card cannot be used in this slot if used with a high-density EIA or in a 1:N configuration.
5. EC1 cards cannot be used in this slot if used with a high-density EIA.

Stop. You have completed this procedure.

DLP-A36 Install the TCC2 Cards

Purpose	This task installs redundant TCC2 cards. The first card you install in the ONS 15454 must be a TCC2 card, and it must initialize before you install any cross-connect or traffic cards.
Tools/Equipment	Two TCC2 cards
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note When installing cards, allow each card to boot completely before installing the next card.

Step 1 Open the latches/ejectors of the first TCC2 card that you will install.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 7 or 11).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

If you insert a card into a slot provisioned for a different card, all LEDS turn off.

Step 4 Verify the LED activity of the TCC2 card:

- All LEDs turn on briefly.
- The red FAIL LED, the yellow ACT/STBY LED, the red REM LED, the green SYNC LED, and the green ACO LED turn on and remain on for about 10 seconds.
- The red FAIL LED and the green ACT/STBY LED turn on and remain on for about 40 seconds.
- The red FAIL LED blinks for about 10 seconds.
- The red FAIL LED turns on for about 5 seconds.
- Both green PWR LEDs turn on for 5 seconds. The PWR LEDs then turn red for 2 to 3 minutes before going to steady green.
- All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for about 10 seconds.
- The ACT/STBY LED turns on. (The ACT/STBY LED might take several minutes to turn on while the DCC processor boots.)

Note It may take up to 3 minutes for the A and B power alarms to clear.

Note If the FAIL LED is on continuously, see the tip below about the TCC2 card automatic upload.

Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

Step 5 Verify that the ACT/STBY LED is green for active. The IP address, temperature of the node, and time of day appear on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Step 6 The LCD cycles through the IP address, node name, and software version. Verify that the correct software version displays on the LCD.

Step 7 If the LCD shows the correct software version, continue with Step 8. If the LCD does not show the correct software version, upgrade the software or remove the TCC2 card and install a replacement card.

Refer to the *Cisco ONS 15454 Software Upgrade Guide* to replace the software. To exchange the TCC2 card, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Open the latches/ejectors of the redundant TCC2 card.

Step 9 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 7 or 11).

Step 10 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 11 Verify the LED activity of the redundant TCC2 card:

- All LEDs turn on briefly.
- The red FAIL LED, the yellow ACT/STBY LED, the red REM LED, the green SYNC LED, and the green ACO LED turn on for about 10 seconds.
- The red FAIL LED and the green ACT/STBY LED turn on for about 40 seconds.
- The red FAIL LED blinks for about 10 seconds.
- The red FAIL LED turns on for about 5 seconds.
- All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for about 10 seconds.
- The ACT/STBY LED turns on. (The ACT/STBY LED might take several minutes to turn on while the DCC processor boots.)

Tip If you install a standby TCC2 card that has a different software version than the active TCC card, the newly installed standby TCC2 card automatically copies the software version from the active TCC2 card. You do not need to do anything in this situation. However, the loading TCC2 card does not boot up in the normal manner. When the standby card is first inserted, the LEDs follow most of the sequence listed in Step 11. After the red FAIL LED turns on for about 5 seconds, the FAIL LED and the ACT/STBY LED begin to flash alternately for up to 30 minutes while the new software loads onto the active TCC2 card. After loading the new software the upgraded TCC2 card's LEDs repeat the sequence from Step 11, and the amber ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDS turn off.

Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

Step 12 Verify that the ACT/STBY LED is amber for standby.

Step 13 Return to your originating procedure (NTP).

DLP-A37 Install the XC, XCVT, or XC10G Cards

Purpose	This task installs the cross-connect (XC/XCVT/XC10G) cards. Cross-connect cards are not necessary in DWDM-only shelves.
Tools/Equipment	XC/XCVT/XC10G (cross-connect) cards
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	Required in non-DWDM shelves.
Onsite/Remote	Onsite
Security Level	None

Note Do not use this procedure to upgrade cross-connect cards. If you are upgrading an XC card to an XCVT, or an XCVT card to a XC10G, see Chapter 14, "Upgrade Cards and Spans."

Note When installing cards, let each card boot completely before installing the next card.

Step 1 Open the latches/ejectors of the first XC, XCVT, or XC10G card that you will install.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the LED activity:

- The red LED turns on for 20 to 30 seconds.
- The red LED blinks for 35 to 45 seconds.
- The red LED turns on for 5 to 10 seconds.
- All LEDs blink once and turn on.
- The ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDS turn off.

Note If the red FAIL LED does not turn on, check the power.

Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 4.

Step 5 Verify that the ACT/STBY LED is green for active.

Step 6 Use the latches/ejectors to firmly slide the second cross-connect card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

Step 7 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 8 Verify the LED activity:

- The red LED turns on for 20 to 30 seconds.
- The red LED blinks for 35 to 45 seconds.
- The red LED turns on for 5 to 10 seconds.
- All LEDs blink once and turn on.
- The ACT/STBY LED turns on.

Note If you insert a card into a slot provisioned for a different card, all LEDS turn off.

Note If the red FAIL LED does not turn on, check the power.

Note If the red FAIL LED is turned on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 6 through 8.

Step 9 Verify that the ACT/STBY LED is amber for standby.

Step 10 Return to your originating procedure (NTP).

DLP-A38 Install the Alarm Interface Controller or Alarm Interface Controller–International Card

Purpose	This task installs the AIC or AIC-I card. The AIC or AIC-I card provides connections for external alarms and controls (environmental alarms).
Tools/Equipment	AIC or AIC-I card
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7 DLP-A37 Install the XC, XCVT, or XC10G Cards, page 2-9 for TDM and hybrid nodes
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note When installing cards, allow each card to boot completely before installing the next card.

Step 1 Open the latches/ejectors on the card.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 9).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 If you have installed the AIC card, verify the following:

- The red FAIL LED turns on for 1 second, then blinks for 1 to 5 seconds.
- After 1 to 5 seconds, all LEDs blink once and turn off.
- The ACT LED turns on.

Step 5 If you have installed the AIC-I card, verify the following:

- The red FAIL LED turns on for 1 second, then blinks for 1 to 5 seconds.
- The PWR A and PWR B LEDs become red and the two INPUT/OUTPUT LEDs become green for approximately 3 seconds.
- The PWR A LED turns green, the INPUT/OUTPUT LEDs turn off, and the ACT LED turns on.

Note It may take up to 3 minutes for the PWR A and PWR B LEDs to update.

Note If the red FAIL LED does not turn on, check the power.

Note If you insert a card into a slot provisioned for a different card, no LEDs turn on.

Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 5.

Step 6 Return to your originating procedure (NTP).

NTP-A16 Install the OC-N Cards

Purpose	This procedure describes how to install optical (OC-N) cards (OC-3, OC-12, OC-48, and OC-192).
Tools/Equipment	OC-3, OC-12, OC-48, and OC-192 cards (as applicable)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

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

Warning **On all OC-N cards except the OC192 LR/STM64 LH 1550 card, the laser is on even when the optical port is not in service. On the OC192 LR/STM64 LH 1550 card, the laser is active when the card is booted and the safety key is in the on position (labeled 1). The laser is off when the safety key is off (labeled 0).**

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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note To simplify path protection to bidirectional line switch ring (BLSR) conversion and node addition, install OC-N cards according to a high-speed east (Slots 12 and 13) and west (Slots 5 and 6) configuration. This configuration is not mandatory.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Note During the boot process an out-of-service (OOS) OC-N port will output AIS-L to any in-service (IS) far-end receivers . See the *Cisco ONS 15454 Troubleshooting Guide* for further information about the AIS-L condition.

Step 1 If you installed XC or XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Install higher-capacity cards first; for example, install an OC-192 card before installing an OC-48 card. Let each card completely boot before installing the next card.

Step 2 Open the card latches/ejectors.

Warning **Before installing an OC192 LR/STM64 LH 1550 card, make sure the safety key on the faceplate is in off position (labeled 0). When in the on position (labeled 1), the laser is activated.**

Step 3 Use the latches/ejectors to firmly slide the OC-N card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 5 to 10 seconds.
- The ACT or ACT/STBY LED becomes amber. The signal fail (SF) LED can persist until all card ports connect to their far end counterparts and a signal is present.

Step 6 If the card does not boot up properly, or the LED activity does not mimic Step 5, check the following:

- When a physical card type does not match the type of card provisioned for that slot in CTC, the card might not boot. If an OC-N card does not boot, open CTC and ensure that the slot is not provisioned for a different card type before assuming the card is faulty.
- If the red FAIL LED does not turn on, check the power.

- If you insert a card into a slot provisioned for a different card, all LEDS turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 5.

Step 7 Continue with the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Stop. You have completed this procedure.

NTP-A249 Install the Transponder and Muxponder Cards

Purpose	This procedure describes how to install the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G (transponder) and MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards (as applicable)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Class 1 Laser Product.**

Warning **Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.**

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

Caution Always use the supplied 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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Note Cisco recommends that you install transponder and muxponder cards after you install OC-N cards, as applicable.

Step 1 If you installed XC or XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the transponder or muxponder card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 5 to 10 seconds.
- The ACT or ACT/STBY LED turns on. The signal fail (SF) LED can persist until all card ports connect to their far end counterparts and a signal is present.

Step 6 If the card does not boot up properly, or the LED activity does not mirror Step 5, check the following:

- When a physical card type does not match the type of card provisioned for that slot in CTC, the card might not boot. If a transponder or muxponder card does not boot, open CTC and ensure that the slot is not provisioned for a different card type before assuming the card is faulty.
- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot provisioned for a different card, all LEDS turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 5.

Step 7 If you installed an MXP_2.5G_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card, complete the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 8 Continue with the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Stop. You have completed this procedure.

NTP-A17 Install the Electrical Cards

Purpose	This procedure describes how to install electrical cards (DS-1, DS-3, DS3XM-6 and EC-1).
Tools/Equipment	Electrical cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note Install higher-capacity cards first; for example, install a DS-3 card before installing a DS-1 card. Let each card boot completely before installing the next card.

Note If you are installing OC-N, TXP, or MXP cards Cisco recommends that you install these before you install electrical cards, as applicable.

Step 1 If you installed XC or XCVT cards, review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 10 to 15 seconds.
- If the red FAIL LED does not turn on, check the power.
- The red FAIL LED blinks for 30 to 40 seconds.
- All LEDs blink once and turn off for 1 to 5 seconds.
- The ACT or ACT/STBY LED turns on. The SF LED can persist until all card ports connect to their far end counterparts and a signal is present.

Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Note If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 5.

Step 6 Continue with the "NTP-A246 Install Ethernet Cards and Connectors" procedure on page 2-17 if necessary.

Stop. You have completed this procedure.

NTP-A246 Install Ethernet Cards and Connectors

Purpose	This procedure describes how to install the Ethernet cards (E100T-12, E100T-G, E1000-2, E1000-2-G, G1000-4, G1K-4, ML100-T-12, and ML10002).
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

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

Caution Always use the supplied 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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you are installing OC-N, TXP, or MXP cards Cisco recommends that you install these before you install Ethernet cards

Step 1 If you installed XC or XCVT cards review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Complete the "DLP-A39 Install Ethernet Cards" task on page 2-18. Allow each card to boot completely before installing the next card.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 3 Complete the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20 if you are using E1000-2, E1000-2-G, G1000-4, or ML1000-2 cards.

Note If you need to remove a GBIC or SFP, complete the "DLP-A470 Remove GBIC or SFP Connectors" task on page 2-22.

Step 4 Continue with the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-56.

Stop. You have completed this procedure.

DLP-A39 Install Ethernet Cards

Purpose	This task installs the Ethernet cards.
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the card latches/ejectors.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.

> **Note** It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 1 to 5 seconds.
- The ACT or ACT/STBY LED turns on. The SF LED can persist until all card ports connect to their far end counterparts and a signal is present.

> **Note** If the red FAIL LED does not turn on, check the power.

> **Note** If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 5 Return to your originating procedure (NTP).

DLP-A469 Install GBIC or SFP Connectors

Purpose	This task installs gigabit interface converters (required for E-Series Ethernet, G-Series Ethernet, and FC_MR-4 cards) and small-form factor pluggables (SFPs) (required for ML1000-2 and MXP cards) and attaches fiber to the connectors.
Tools/Equipment	For E1000-2-G use: • SX GBIC= for short-reach applications • LX GBIC= for long-reach applications For the G1000-4 or G1K-4 card use: • SX GBIC= for short-reach applications • LX GBIC= for long-reach applications • ZX GBIC= for extra long-reach applications • DWDM GBIC= for DWDM applications For the ML1000-2 card use: • SX SFP= for short-reach applications • LX SFP= for long-reach applications For the MXP card use: • 15454E-SFP-L.16.1= for short-reach applications • ONS-SE-2G-S1= for long-reach applications For the FC_MR-4 card use: • ONS-GX-2FC-SML= (2Gb FC 1310nm Single mode with SC connectors) • ONS-GX-2FC-MMI= (2Gb FC 850nm Multi mode with SC connectors)
Prerequisite Procedures	NTP-A249 Install the Transponder and Muxponder Cards, page 2-14 DLP-A39 Install Ethernet Cards, page 2-18 NTP-A274 Install the FC_MR-4 Cards, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1000-4 cards compatible with DWDM GBICs have a CLEI code of SNP8KW0KAB. Compatible G1K-4 cards have a CLEI code of WM5IRWPCAA.

Note All versions of G1000-4 and G1K-4 cards support CWDM GBICs.

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

Step 1 Remove the GBIC or SFP from its protective packaging.

Step 2 Check the label to verify that the GBIC or SFP is the correct type for your network.

Table 2-3 shows the available GBICs.

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

Table 2-3 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=
	FC_MR-4	Long reach	Single-mode fiber, 1310nm	ONS-GX-2FC-SML=
	FC_MR-4	Intermediate reach	Multi-mode fiber, 850nm	ONS-GX-2FC-MMI=

Table 2-4 shows the available SFPs.

Table 2-4 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=

Step 3 Verify the type of GBIC or SFP you are using:

- If you are using a GBIC with clips, go to Step 4.
- If you are using a GBIC with a handle, go to Step 5.
- If you are using an SFP, go to Step 6.

Step 4 For GBICs with clips:

a. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

Note GBICs are keyed to prevent incorrect installation.

b. Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

c. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

d. Continue with Step 7.

Step 5 For GBICs with a handle:

a. Remove the protective plug from the SC-type connector.

b. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

c. Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to an SC-type connector.

d. Slide the GBIC through the cover flap until you hear a click.

The click indicates that the GBIC is locked into the slot.

e. Continue with Step 7.

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.**

Step 6 For SFPs:

a. Plug the LC duplex connector of the fiber into a Cisco-supported SFP connector.

b. If the new SFP connector has a latch, close the latch over the cable to secure it.

c. Plug the cabled SFP connector into the card port until it clicks.

Step 7 Return to your originating procedure (NTP).

DLP-A470 Remove GBIC or SFP Connectors

Purpose	This task disconnects fiber attached to GBICs or SFPs and removes the GBICs or SFPs.
Tools/Equipment	None
Prerequisite Procedures	DLP-A469 Install GBIC or SFP Connectors, page 2-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

Step 2 If you are using a GBIC with clips:

a. Release the GBIC from the slot by squeezing the two plastic tabs on each side of the GBIC.

b. Slide the GBIC out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Step 3 If you are using a GBIC with a handle:

a. Release the GBIC by opening the handle.

b. Pull the handle of the GBIC.

c. Slide the GBIC out of the Gigabit Ethernet card slot. A flap closes over the GBIC slot to protect the connector on the Gigabit Ethernet card.

Step 4 If you are using an SFP:

a. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

b. Pull the fiber cable straight out of the connector.

c. Unplug the SFP connector and fiber from the card.

d. Slide the SFP out of the Gigabit Ethernet card slot.

Step 5 Return to your originating procedure (NTP).

NTP-A274 Install the FC_MR-4 Cards

Purpose	This procedure installs the Fibre Channel (FC_MR-4) card.
Tools/Equipment	FC_MR-4 card(s)
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

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

Caution Always use the supplied 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 If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Step 1 If you installed XC or XCVT cards review Table 2-1 on page 2-3 to determine card/slot compatibility. If you installed XC10G cards, review Table 2-2 on page 2-5 to determine card/slot compatibility.

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

> **Note** If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57 and install the correct card.

Step 4 Verify that the card is inserted correctly and close the latches/ejectors on the card.

> **Note** It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 5 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds. The ACT LED is amber for 3 to 5 seconds.
- The red FAIL LED blinks for up to 2 minutes.

> **Note** If the red FAIL LED does not turn on, check the power.

- The FAIL and ACT LEDs blink once and turn off for 1 to 5 seconds.
- The ACT LED turns on green to indicate the card is operational.

> **Note** If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 6 Complete the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20 to install GBICs on the FC_MR-4 card.

Note If you need to remove a GBIC or SFP, complete the "DLP-A470 Remove GBIC or SFP Connectors" task on page 2-22.

Step 7 Continue with the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Stop. You have completed this procedure.

NTP-A242 Install the DWDM Cards

Purpose	This procedure describes how to install DWDM cards (OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, or OSC-CSM). Complete this procedure when instructed to do so in Chapter 5, "Turn Up a DWDM Node."
Tools/Equipment	OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, or OSC-CSM cards (as applicable)
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.**

Warning **Class 1M Laser Product.**

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

Caution Always use the supplied 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 Do not install the DWDM cards until you are directed to do so during DWDM node turnup.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If you install a card incorrectly, the FAIL LED flashes continuously.

Note The automatic node setup (ANS) of the ONS 15454 DWDM system begins to determine what kind of site you are installing as soon as you install cards. The automatic power control (APC) is enabled after ANS initializes and after a channel has been provisioned. To provision a DWDM channel, see the "NTP-A227 Provision a DWDM Optical Channel Network Connection" procedure on page 8-98. For more information about amplifier power control, see the *Cisco ONS 15454 Reference Manual*.

Step 1 Plan your node installation or consult the site plan. As soon as you begin installing cards, ANS determines what kind of site to set up based on the following parameters:

- Hub site—Two 32DMX-O and two 32MUX-O cards are provisioned but no AD-xC or AD-xB cards are provisioned
- Terminal—One 32DMX-O and one 32MUX-O card are provisioned, and no AD-xC or AD-xB cards are provisioned
- Line site—Only one OPT-PRE or OPT-BST is provisioned per line direction. (Up to two OPT-PRE and/or two OPT-BST cards can be provisioned in the same shelf.)
- OADM site—At least 1 AD-xC or AD-xB is provisioned and no 32DMX-O or 32MUX-O cards are provisioned
- Unknown—Provisioned cards do not follow any of the previously listed categories

Step 2 Open the card latches/ejectors.

Step 3 Use the latches/ejectors to firmly slide the DWDM card along the guide rails until the card plugs into the receptacle at the back of the slot.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57 and install the correct card.

Step 4 Use the following card placement guidelines. For specific information about each card, refer to the *Cisco ONS 15454 Reference Manual*.

- OPT-BST cards can be installed in any open east and west pair of slots but are often installed in Slots 1 and 17.
- OPT-PRE cards can be installed in any open east and west pair of slots but are often installed in Slots 2 and 16.
- OSCM cards, if used, are installed in Slots 8 and 10.
- OSC-CSM cards, if used (when there is no OPT-BST), can be installed in any open east and west pair of slots.

- 32MUX-O cards are double-slot cards and are often installed in Slots 3 and 4 and Slots 14 and 15.
- 32DMX-O cards are double-slot and are often installed in Slots 5 and 6 and Slots 12 and 13.
- AD cards (channel or band) and 4MD-xx.x combiner cards are installed in any open slots.

Note Refer to Figures 2-8, 2-9, 2-10, and 2-11 to see typical site shelf diagrams that contain cards and show cabling schemes.

Step 5 Verify that the card is inserted correctly and close the latches/ejectors on the card.

Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 6 Verify the LED activity:

- The FAIL LED turns on for approximately 35 seconds
- The FAIL LED blinks for approximately 40 seconds
- All LEDs turn on and then turn off within 5 seconds
- If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type
- The ACT LED turns on
- The signal fail (SF) LED stays on until all card ports connect to their far-end counterparts and a signal is present

Step 7 If the card does not boot up properly, or the LED activity does not mimic Step 5, check the following:

- When a physical card type does not match the type of card provisioned for that slot in CTC, the card might not boot. If a DWDM card does not boot, open CTC and ensure that the slot is not provisioned for a different card type before assuming the card is faulty.
- If the red FAIL LED does not turn on, check the power.
- If you insert a card into a slot provisioned for a different card, all LEDS turn off.
- If the red FAIL LED is on continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 to 6.

Step 8 If you installed OPT-PRE cards, complete the "NTP-A243 Install the DWDM Dispersion Compensating Cards" procedure on page 2-28.

Step 9 Complete the "NTP-A244 Install Fiber-Optic Cables on DWDM Cards" procedure on page 2-41.

Stop. You have completed this procedure.

NTP-A243 Install the DWDM Dispersion Compensating Cards

Purpose	This procedure describes how to install the dispersion compensating cards (DCU-xx.x) for DWDM shelves and is required if OPT-PRE cards are installed. Required if the span is very long. If Metroplanner is used to generate the bill of materials, the need for DCUs will be indicated. Complete this procedure when instructed to do so in Chapter 5, "Turn Up a DWDM Node."
Tools/Equipment	DCU-xx.x cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2 NTP-A242 Install the DWDM Cards, page 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool due to electrical hazard.**

Warning **Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.**

Warning **Class 1M laser product.**

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

Caution Always use the supplied 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 Do not install the DWDM cards until you are directed to do so during DWDM node turnup.

Note If protective clips are installed on the backplane connectors of the cards, remove the clips before installing the cards.

Note If a DCU is not required, a 4 dB optical attenuated patch cord must be placed between the OPT-PRE DCC Tx and Tx ports.

Step 1 Pull the card latch inward with your finger.

Step 2 Firmly slide the DCU card along the guide rails until the card plugs into the receptacle at the back of the horizontal dispersion compensating card slots at the top of the shelf.

Note The West dispersion compensating card is commonly installed on the left side and the East card is commonly installed on the right.

Note If you install the wrong card in a slot, complete the "NTP-A116 Remove and Replace a Card" procedure on page 2-57 and install the correct card.

Step 3 Release the finger latch.

Note It is possible to close the latch when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify that the card is engaged with the backplane by grasping and gently pulling the card handle. If the card does not move, it is fully installed. If it moves, repeat Step 2.

Step 5 Continue with the "NTP-A244 Install Fiber-Optic Cables on DWDM Cards" procedure on page 2-41.

Stop. You have completed this procedure.

NTP-A247 Install Fiber-Optic Cables on OC-N Cards

Purpose	This procedure describes how to install fiber-optic cables on OC-N cards or GBICs according to topology.
Tools/Equipment	Fiber-optic cables
	Fiber boot
Prerequisite Procedures	NTP-A16 Install the OC-N Cards, page 2-12
	NTP-A249 Install the Transponder and Muxponder Cards, page 2-14 (if applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

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

Warning **On all OC-N cards except the OC192 LR/STM64 LH 1550 card, the laser is on even when the optical port is not in service. On the OC192 LR/STM64 LH 1550 card, the laser is active when the card is booted and the safety key is in the on position (labeled 1). The laser is off when the safety key is off (labeled 0).**

Warning **Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector.**

Caution Do not use fiber loopbacks with the OC192 LR/STM64 LH 1550 or OC192 LR/STM64 LH ITU 15xx.xx card unless you are using a 20-dB attentuator. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC192 LR/STM64 LH 1550 or OC192 LR/STM64 LH ITU 15xx.xx card.

Caution Do not use fiber loopbacks with the OC192 IR/STM64 SH 1550 card unless you are using a 5-dB attentuator. Never connect a direct, unattenuated fiber loopback. Using unattenuated fiber loopbacks causes irreparable damage to the OC192 IR/STM64 SH 1550 card.

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 Fiber boots are not recommended for OC192 cards or OC48AS cards because of the downward angle of the optical ports.

Note You can install the fiber immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 6, "Turn Up Network."

Step 1 Test the optical receive levels for the cards installed and attenuate accordingly. See Table 2-5 for the minimum and maximum levels.

Table 2-5 OC-N Card Transmit and Receive Levels

Card	Transmit		Receive	
	Minimum	Maximum	Minimum	Maximum
OC3 IR 4/STM1 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC3IR/STM1SH 1310-8	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1310	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1550	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310-4	–15 dBm	–8 dBm	–30 dBm	–8 dBm
OC48 IR 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm
OC48 IR/STM16 SH AS 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR/STM16 LH AS 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm
OC48 ELR/STM16 EH 100 GHz	–2 dBm	0 dBm	–27 dBm at 1E-12 BER	–9 dBm
OC48 ELR/STM16 EH 200 GHz	–2 dBm	0 dBm	–28 dBm	–8 dBm
OC192 SR/STM64 IO 1310	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192 IR/STM64 SH 1550	–1 dBm	+2 dBm	–14 dBm	–1 dBm
OC192 LR/STM64 LH 1550	+7 dBm	+10 dBm	–19 dBm	–10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	+3 dBm	+6 dBm	–22 dBm	–9 dBm
TXP_MR_10G (trunk side)	–16 dBm[1]	+3 dBm[1]	–24 dBm	–8 dBm
TXP_MR_10G (client side)	–6 dBm	–1 dBm	–14 dBm	–1 dBm
MXP_2.5G_10G (trunk side)	–16 dBm[1]	+3 dBm[1]	–24 dBm	–8 dBm
MXP_2.5G_10G (client side)	–5 dBm	0 dBm	depends on SFP	depends on SFP
TXP_MR_2.5G (trunk side) TXPP_MR_2.5G (trunk side)	–16 dBm	+3 dBm	depends on forward error correction (FEC)	depends on FEC
TXP_MR_2.5G (client side) TXPP_MR_2.5G (client side)	–6 dBm	–1 dBm	–14 dBm at 1E-12 BER	–1 dBm at 1E-12 BER

1. On transponder and muxponder cards, the optical output power on the trunk side can be configured from –16 to +3 dBm with an accuracy of +/–0.5 dB.

Step 2 Inspect and clean all fiber connectors thoroughly. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 3 As needed, complete the "DLP-A207 Install Fiber-Optic Cables on the LGX Interface" task on page 2-32.

Step 4 Complete the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 2-33.

Note To install fiber-optic cables on Ethernet cards, FC_MR-4 cards, or transponder/muxponder cards, see the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 5 As needed, complete the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task on page 2-34.

Step 6 As needed, complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-37.

Step 7 As needed, complete the "DLP-A45 Install the Fiber Boot" task on page 2-39.

Step 8 Continue with the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-56.

Stop. You have completed this procedure.

DLP-A207 Install Fiber-Optic Cables on the LGX Interface

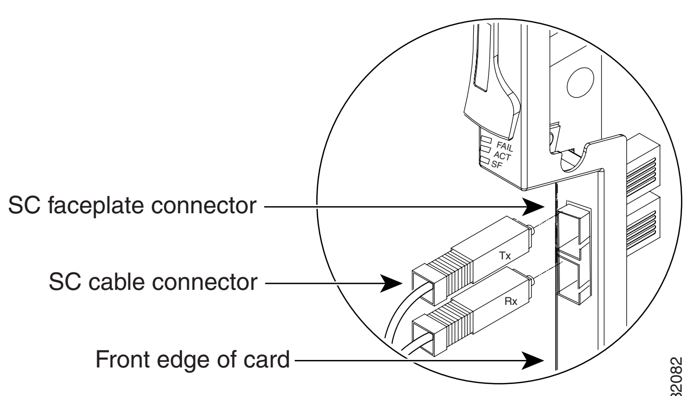
Purpose	This task installs fiber-optic cables on the Lightguide Cross Connect (LGX) interface in the Central Office.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the keyed ridge of the cable connector with the receiving SC connector on the LGX faceplate connection point. Each module supports at least one transmit and one receive connector to create an optical carrier port.

Step 2 Gently insert the cable connector into the faceplate connection point until the connector snaps into place.

Step 3 Connect the fiber optic cable to the OC-N card. Figure 2-1 shows the cable location.

Figure 2-1 Installing Fiber-Optic Cables



Step 4 Return to your originating procedure (NTP).

DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration

Purpose	This task installs fiber-optic cables on optical (OC-N) cards in a 1+1 linear configuration.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The Cisco OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics, all working at 1310 nm, are optimized for the most widely used SMF-28 fiber, available from many suppliers.

Note Corning MetroCor fiber is optimized for optical interfaces that transmit at 1550 nm or in the C and L DWDM windows. This fiber targets interfaces with higher dispersion tolerances than those found in OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics. If you are using Corning MetroCor fiber, OC-3 IR/STM-1 SH, OC- 12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics will become dispersion limited before they will become attenuation limited. In this case, consider using OC-3 LR/STM-1 LH, OC-12 LR/STM-4 LH, and OC-48 LR/STM-16 LH cards instead of OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH cards.

Note With all fiber types, network planners/engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

Step 1 Plan your fiber connections. Use the same plan for all 1+1 nodes.

Step 2 Align the keyed ridge of the cable connector with the transmit (Tx) connector of a working OC-N card at one node and plug the other end of the fiber into the receive (Rx) connector of a working OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports). Figure 2-1 on page 2-32 shows the cable location.

Step 3 Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and all other working/protect port pairs you want to place in a 1+1 configuration.

Step 4 Return to your originating procedure (NTP).

DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations

Purpose	This task connects the fiber-optic cables to the east and west path protection ports at each node. See Chapter 6, "Turn Up Network" to provision and test path protection configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Caution Do not provision the path protection east and west ports on the same OC-N card.

Step 1 Plan your fiber connections. Use the same plan for all path protection nodes.

Step 2 Plug the fiber into the transmit (Tx) connector of an OC-N card at one node and plug the other end of the fiber into the receive (Rx) connector of an OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have configured the ring.

Figure 2-2 shows fiber connections for a four-node path protection with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 2-2 Connecting Fiber to a Four-Node Path Protection

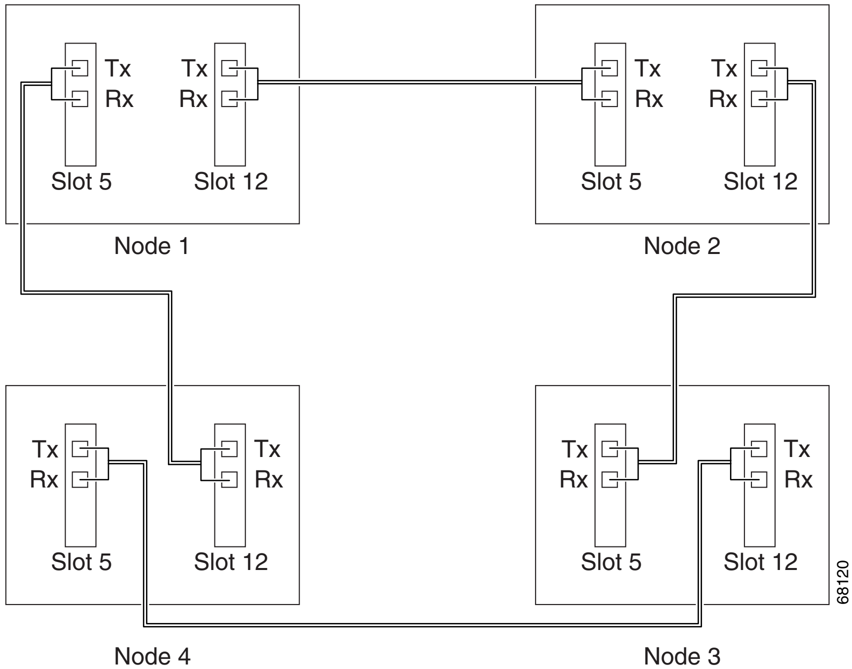


Figure 2-3 shows a traditional path protection dual ring interconnect example.

Figure 2-3 Connecting Fiber to an Eight-Node Traditional Path Protection Dual-Ring Interconnect

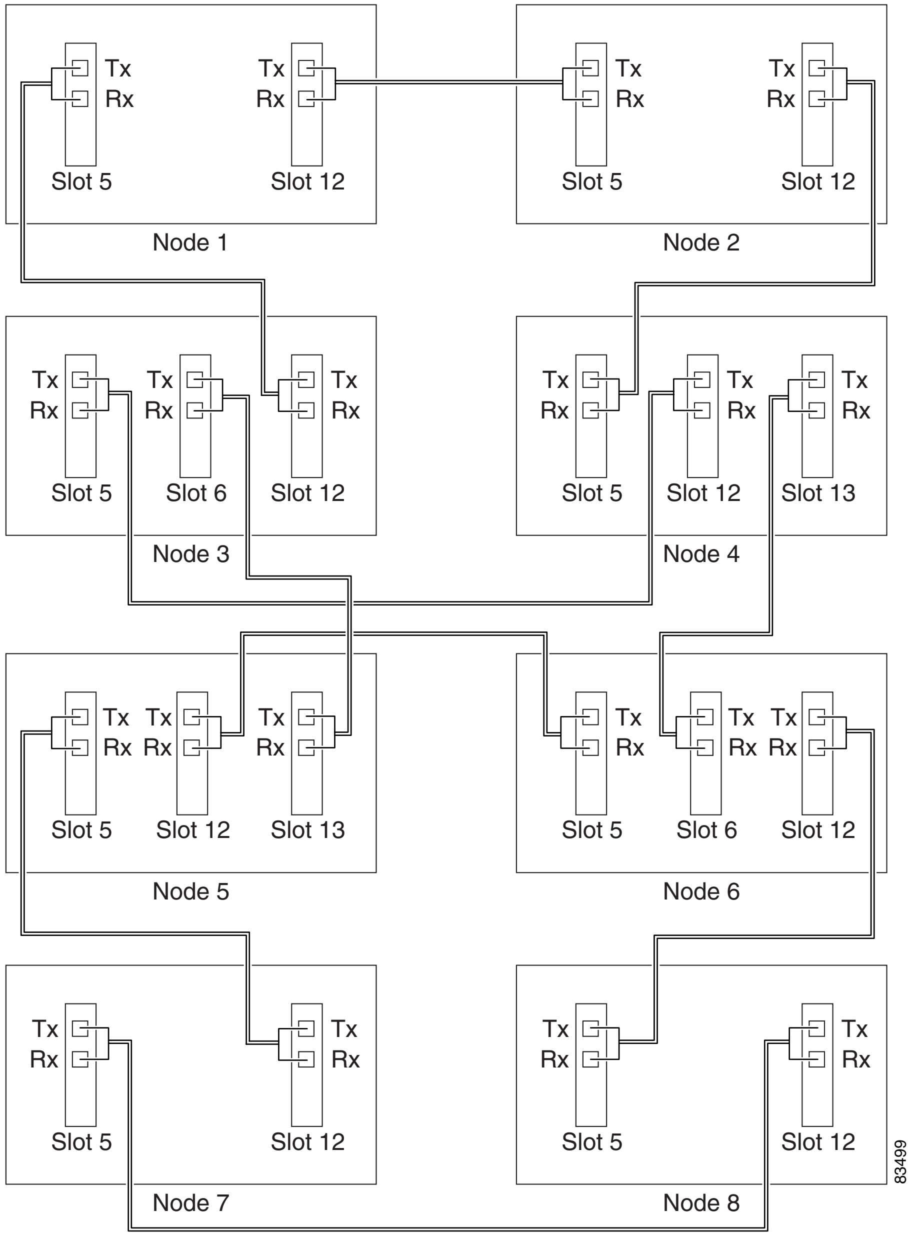
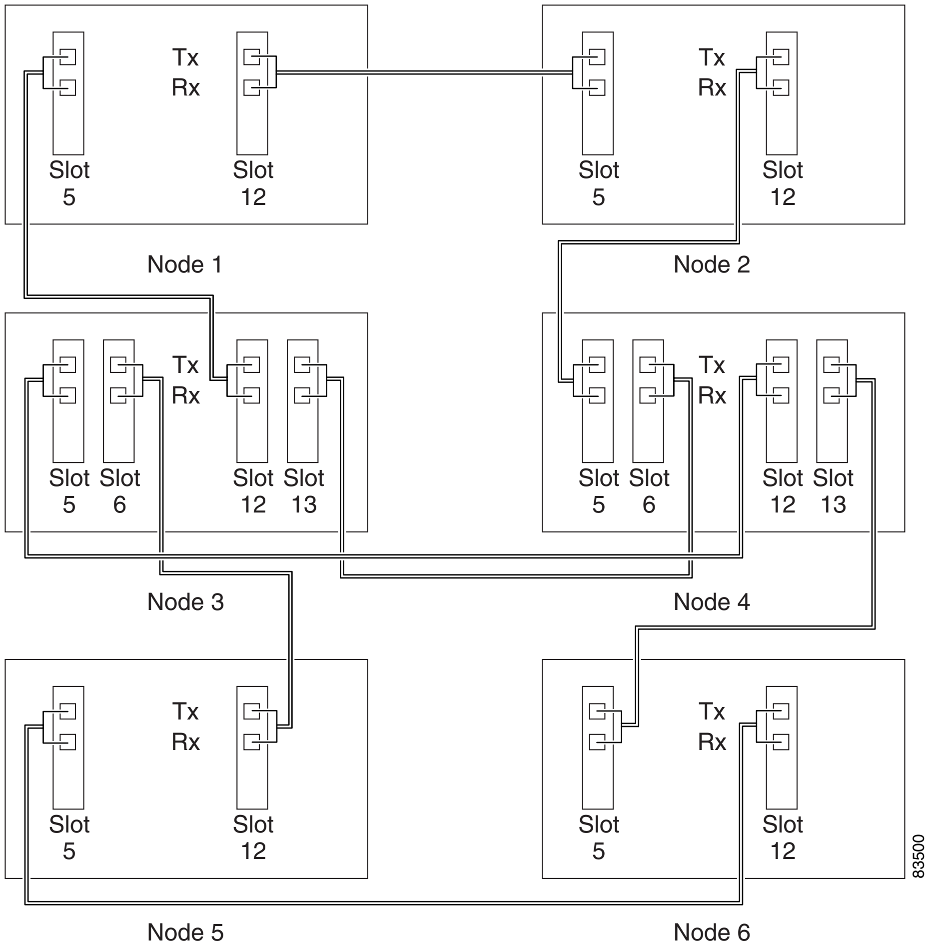


Figure 2-4 shows an integrated dual ring interconnect example.

Figure 2-4 Connecting Fiber to a Six-Node Integrated Path Protection Dual-Ring Interconnect



Step 4 Return to your originating procedure (NTP).

DLP-A44 Install Fiber-Optic Cables for BLSR Configurations

Purpose	This task installs the fiber-optics to the east and west BLSR ports at each node. See Chapter 6, "Turn Up Network" to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Caution Do not provision the BLSR east and west ports on the same OC-N card.

Step 1 Plan your fiber connections. Use the same plan for all BLSR nodes.

Step 2 Plug the fiber into the transmit (Tx) connector of an OC-N card at one node and plug the other end into the receive (Rx) connector of an OC-N card at the adjacent node. The card displays a SF LED if the transmit and receive fibers are mismatched.

Note Do not mix working and protect card connections when connecting a four-fiber BLSR. The BLSR does not function if working and protect cards are interconnected. See Figure 2-6 on page 2-39 for an example of correct four-fiber BLSR cabling.

Step 3 Repeat Step 2 until you have configured the ring.

Figure 2-5 shows fiber connections for a two-fiber BLSR with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 2-5 Connecting Fiber to a Four-Node, Two-Fiber BLSR

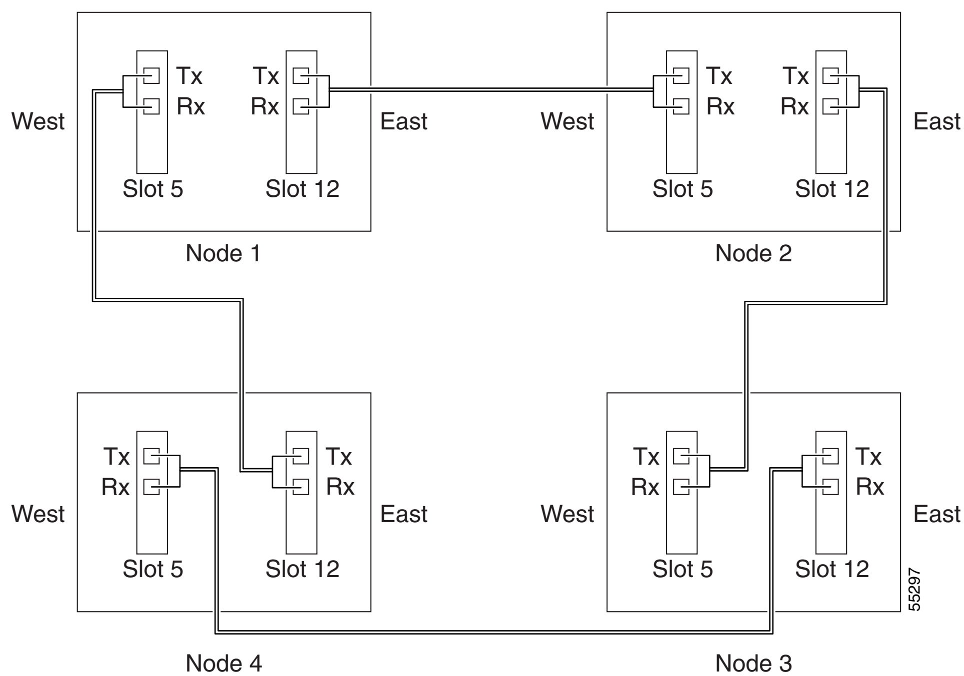
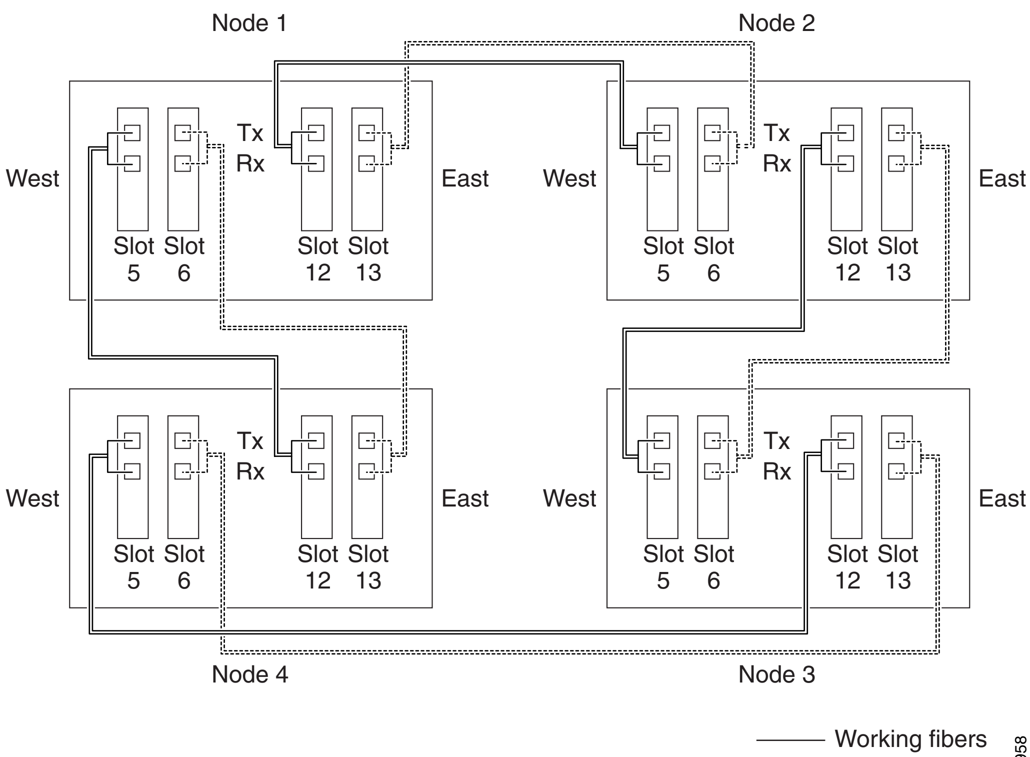


Figure 2-6 shows fiber connections for a four-fiber BLSR. Slot 5 (west) and Slot 12 (east) carry the working traffic. Slot 6 (west) and Slot 13 (east) carry the protect traffic.

Figure 2-6 Connecting Fiber to a Four-Node, Four-Fiber BLSR



Step 4 Return to your originating procedure (NTP).

DLP-A45 Install the Fiber Boot

Purpose	This task installs the fiber boot, which protects the fiber from excessive bending. Required for all OC-N cards except the OC-192 and the OC-48 AS
Tools/Equipment	Fiber boot
Prerequisite Procedures	NTP-A16 Install the OC-N Cards, page 2-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note You can install the fiber boots on the fiber-optic cables before or after the fibers are attached to the OC-N card.

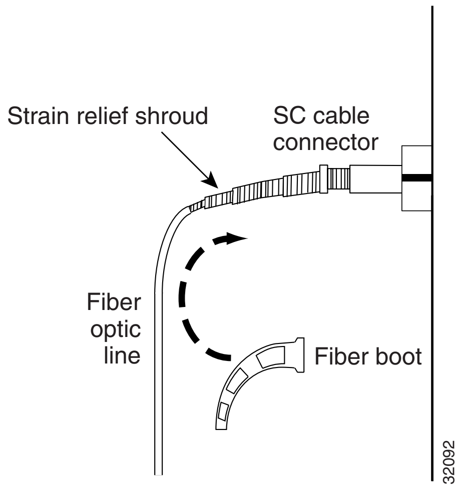
Note The fiber boot does not support the OC-48 IR/STM-16 SH AS 1310, OC-48 LR/STM-16 LH AS 1550, and OC-192 LR/STM64 LH 1550 cards. The boots are not necessary for these cards because of the angled SC connectors on the cards.

Note If you are installing an OC3IR/STM1SH 1310-8 card, you must use a fiber clip instead of a fiber boot on the port 8 Rx fiber connector.

Step 1 Position the open slot of the fiber boot underneath the fiber cable.

Step 2 Push the fiber cable down into the fiber boot. Figure 2-7 shows the fiber boot attachment.

Figure 2-7 Attaching a Fiber Boot



Step 3 Twist the fiber boot to lock the fiber cable into the tail end of the fiber boot.

Step 4 Slide the fiber boot forward along the fiber cable until the fiber boot fits snugly onto the end of the SC cable connector.

Step 5 Return to your originating procedure (NTP).

NTP-A244 Install Fiber-Optic Cables on DWDM Cards

Purpose	This procedure installs the fiber-optic cables to DWDM cards and dispersion compensating cards. The CTC automatic node setup (ANS) feature calculates and provisions the power settings between cards and nodes. This application depends on the presence of correct cabling. See Chapter 7, "Turn Up DWDM Network" to provision and test DWDM configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A242 Install the DWDM Cards, page 2-25 NTP-A243 Install the DWDM Dispersion Compensating Cards, page 2-28 (as applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.**

Warning **Class 1M laser product.**

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Check the optical receive levels for the cards installed and attenuate accordingly. See Table 2-6 for DWDM card minimum and maximum transmit and receive levels. Power levels must be within the acceptable range for that card.

Table 2-6 DWDM Card Transmit and Receive Levels

Card	Transmit		Receive	
	Minimum	Maximum	Minimum	Maximum
32DMX-O (DWDM Channels side)	–29dBm	–8dBm	+2dBm	+17dBm
32MUX-O (DWDM Channels side)	–13dBm	+2dBm	–4.5dBm	+6dBm
4MD-xx.x (DWDM Channels side)	–29 dBm	–8dBm	–4.5dBm	+6dBm
AD-1C-xx.x (DWDM Channels side)	–29dBm	–8dBm	–4.5dBm	+6dBm
AD-2C-xx.x (DWDM Channels side)	–29dBm	–8dBm	–4.5dBm	+6dBm

Table 2-6 DWDM Card Transmit and Receive Levels (continued)

Card	Transmit		Receive	
AD-4C-xx.x (DWDM Channels side)	–29dBm	–8dBm	–4.5dBm	+6dBm
AD-1B-xx.x (DWDM Bands side)	–29dBm	–8dBm	–4.5dBm	+6dBm
AD-4B-xx.x (DWDM Channels side)	–29dBm	–8dBm	–4.5dBm	+6dBm
OSCM (DWDM Channels side)	–24dBm	–0.5dBm	–42dBm	–7dBm

Step 2 Inspect and clean all fiber connectors thoroughly. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 3 Complete the "DLP-A423 Install Fiber-Optic Cables for OSC Link Termination on All DWDM Nodes" task on page 2-42.

Step 4 As required, complete the "DLP-A424 Install Fiber-Optic Cables for a Terminal Node" task on page 2-44.

Step 5 As required, complete the"DLP-A425 Install Fiber-Optic Cables for a Hub Node" task on page 2-45.

Step 6 As required, complete the "DLP-A426 Install Fiber-Optic Cables for a Line Amplifier Node" task on page 2-47.

Step 7 As required, complete the "DLP-A427 Install Fiber-Optic Cables for an Amplified or Passive OADM Node" task on page 2-50.

Step 8 Continue with the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-56.

Stop. You have completed this procedure.

DLP-A423 Install Fiber-Optic Cables for OSC Link Termination on All DWDM Nodes

Purpose	This task explains how to install fiber-optic cables for optical service channels creation on all DWDM shelves.
Tools	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Refer to your site plan when cabling the node. Connect fiber optic cabling for the OSC by consulting the following rules:

- The OPT-BST and the OSC-CSM are the only cards that directly interface with the line (span) fiber.
- The OSCM only carries supervision channels, not DWDM channels.
- The OSCM and the OSC-CSM cannot both be used on the same side of the NE (such as both being on the west side). You can have different cards on each side, for example an OSCM on the west side and an OSC-CSM on the east side.
- When an OPT-BST and an OSC-CSM are both used on the same side of an NE, the OPT-BST combines the supervision channel with the DWDM channels and the OSC-CSM acts as an OSCM; it does not carry DWDM traffic.
- When an OPT-BST and an OSC-CSM are used on opposite sides of the NE, the supervision channel does not require any additional connection.
- The East OPT-BST OSC Rx port is connected to the East OSCM Tx port.
- The East OPT-BST OSC Tx port is connected to the East OSCM Rx port.
- The East OPT-BST OSC Rx port is connected to the East OSC-CSM Line Tx port.
- The East OPT-BST OSC Tx port is connected to the East OSC-CSM Line Rx port.
- The West OPT-BST OSC Tx port is connected to the West OSCM Rx port.
- The West OPT-BST OSC Rx port is connected to the West OSCM Tx port.
- The West OPT-BST OSC-Tx port is connected to the West OSC-CSM Line Rx port.
- The West OPT-BST OSC-Rx port is connected to the West OSC-CSM Line Tx port.

Step 2 Plug the fiber into the West Line transmit (Rx) connector of an OPT-BST (or OSC-CSM) card and into the adjacent node East OPT-BST or OSC-CSM Line Tx connector. Repeat in the other direction (east to west, Rx to Tx). Ensure that you are connecting the West Line ports to the adjacent node East Line ports.

> **Note** The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have connected the nodes according to the site plan.

Step 4 At the West side of the first node, plug one end of a fiber cable into the West OPT-BST OSC Rx connector and the other end into West OSCM Tx connector. Repeat the cabling from the West OSCM Rx to the OPT-BST OSC Tx.

> **Note** An OSC-CSM card takes the place of an OPT-BST and OSCM card for that side of the node and does not require OSC cabling.

Step 5 At the East side of the first node, plug one end of a fiber cable into the East OPT-BST OSC Rx connector and the other end into East OSCM Tx connector. Repeat the cabling from the East OSCM Rx to the OPT-BST OSC Tx.

Step 6 Repeat Steps 4 and 5 at each node.

Step 7 Return to your originating procedure (NTP).

DLP-A424 Install Fiber-Optic Cables for a Terminal Node

Purpose	This task installs fiber-optic cables on a terminal node DWDM shelf. See Chapter 7, "Turn Up DWDM Network" to provision and test DWDM configurations.
Tools	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Refer to your site plan when cabling the node. Connect fiber-optic cabling for the terminal site by consulting the following rules:

- A terminal site has only one side (as compared to a hub node, which has two sides).
- The port line direction is not significant.
- The OPT-BST and OPT-PRE cards are not mandatory.
- The OSC-CSM or OPT-BST COM Tx port is connected to the OPT-PRE COM Rx port or the 32 DMX-O COM Rx port.
- The OPT-PRE COM Tx port is connected to the 32DMX-O COM Rx port.
- The 32MUX-O Tx port is connected to the OSC-CSM or OPT-BST COM Rx port.

Step 2 Plug one fiber cable end into the desired Rx port and other end into the desired Tx port.

Note The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have connected the nodes according to the site plan.

Step 4 Return to your originating procedure (NTP).

DLP-A425 Install Fiber-Optic Cables for a Hub Node

Purpose	This task installs fiber-optic cables on a hub node DWDM shelf. See Chapter 7, "Turn Up DWDM Network" to provision and test DWDM configurations.
Tools	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

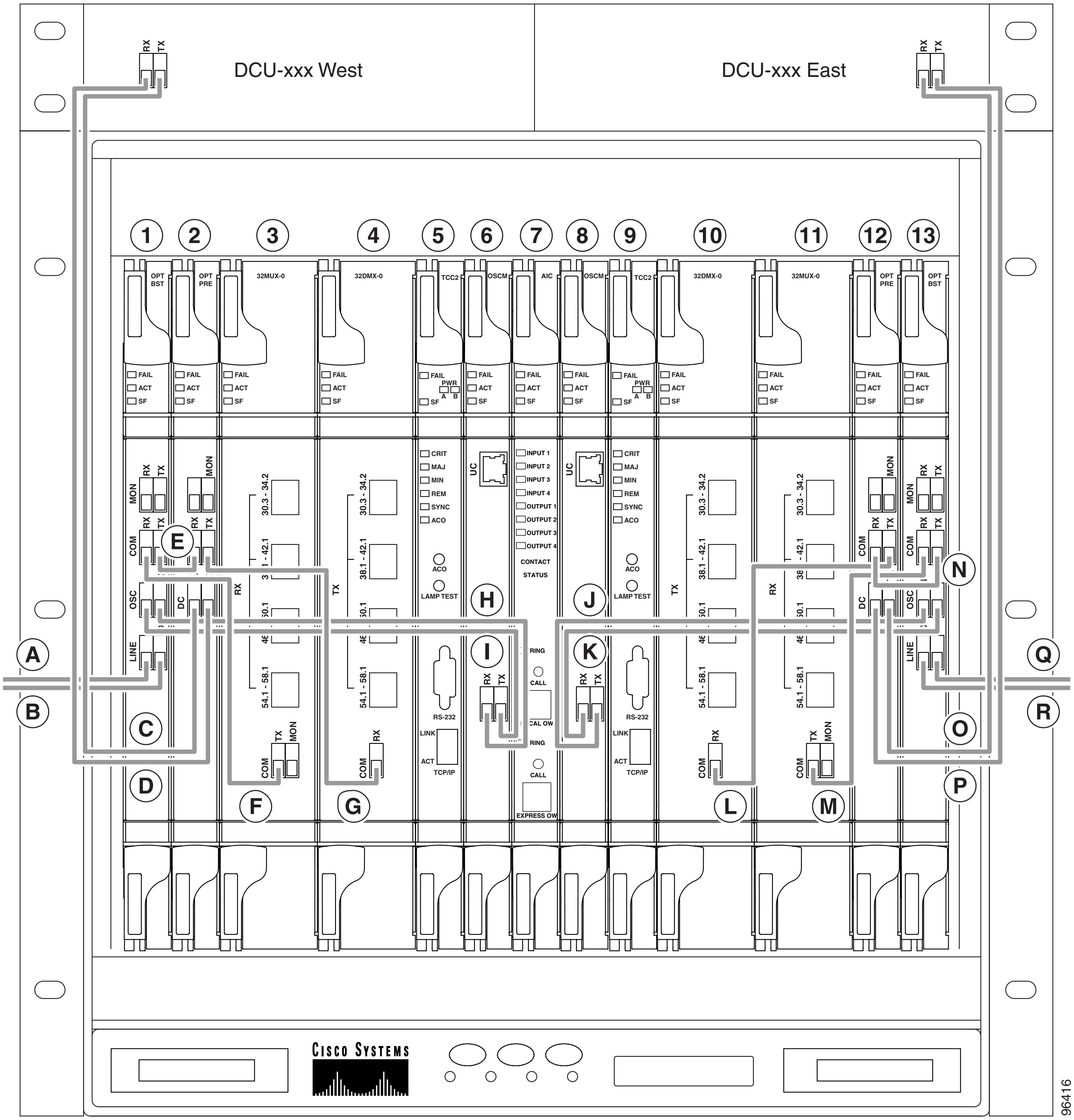
Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Refer to your site plan when cabling the node. Connect fiber optic cabling for the hub node by consulting the following rules:

- The West OPT-BST or OSC-CSM card common (COM) Tx port is connected to the West OPT-PRE COM Rx port or West 32 DMX-O COM Rx port.
- The West OPT-PRE COM Tx port is connected to the West 32DMX-O COM Rx port.
- West 32MUX-O COM Tx port is connected to the West OPT-BST or OSC-CSM COM Rx port.
- The East 32MUX-O COM Tx port is connected to the East OPT-BST or OSC-CSM COM Rx port.
- The East OPT-BST or OSC-CSM COM Tx port is connected to the East OPT-PRE COM Rx port or East 32DMX-O COM Rx port.
- The East OPT-PRE COM Tx port is connected to the 32DMX-O COM Rx port.

Figure 2-8 shows an example of a hub node with cabling.

Figure 2-8 Fibering a Hub Node



1	Slot 1OPT-BST West	**D**	DC West Rx from Slot 2 DCC Tx
2	Slot 2 OPT-PRE West	**E**	Slot 1 COM Tx to Slot 2 COM Rx
3	Slot 3-4 32 MUX-O West	**F**	Slot 1 COM Rx from Slot 3-4 COM Tx
4	Slot 5-6 32 DMX-O West	**G**	Slot 2 COM Tx to Slot 5-6 COM Rx
5	Slot 7 TCC2	**H**	Slot 1 OSC Tx to slot 8 Rx

6	Slot 8 OSCM West	**I**	Slot 1 OSC Rx from Slot 8 Tx
7	Slot 9 AIC	**J**	Slot 10 Tx to Slot 17 OSC Rx
8	Slot 10 OSCM East	**K**	Slot 10 Rx from Slot 17 OSC Tx
9	Slot 11 TCC2	**L**	Slot 12-13 COM Rx from Slot 16 COM Tx
10	Slot 12-13 32 DMX-O East	**M**	Slot 14-15 COM Tx to Slot 17 COM Rx
11	Slot 14-15 32 MUX-O East	**N**	Slot 16 COM Rx from Slot 17 COM Tx
12	Slot 16 OPT-PRE East	**O**	Slot 16 DC Tx to DCU East Rx
13	Slot 17 OPT-BST East	**P**	Slot 16 DC Rx from DCU East Tx
A	Slot 1 Line Rx from span fiber	**Q**	Slot 17 Line Tx to span fiber
B	Slot 1 Line Tx to span fiber	**R**	Slot 17 Line Rx from span fiber
C	DCU West Tx to Slot 2 DC Rx	—	

Step 2 Plug one end of the fiber cable into the desired Rx port and other end into the desired Tx port.

Note The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have connected the nodes according to the site plan.

Step 4 Return to your originating procedure (NTP).

DLP-A426 Install Fiber-Optic Cables for a Line Amplifier Node

Purpose	This task installs fiber-optic cables on a line amplifier node in a DWDM shelf. See Chapter 7, "Turn Up DWDM Network" to provision and test DWDM configurations.
Tools	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

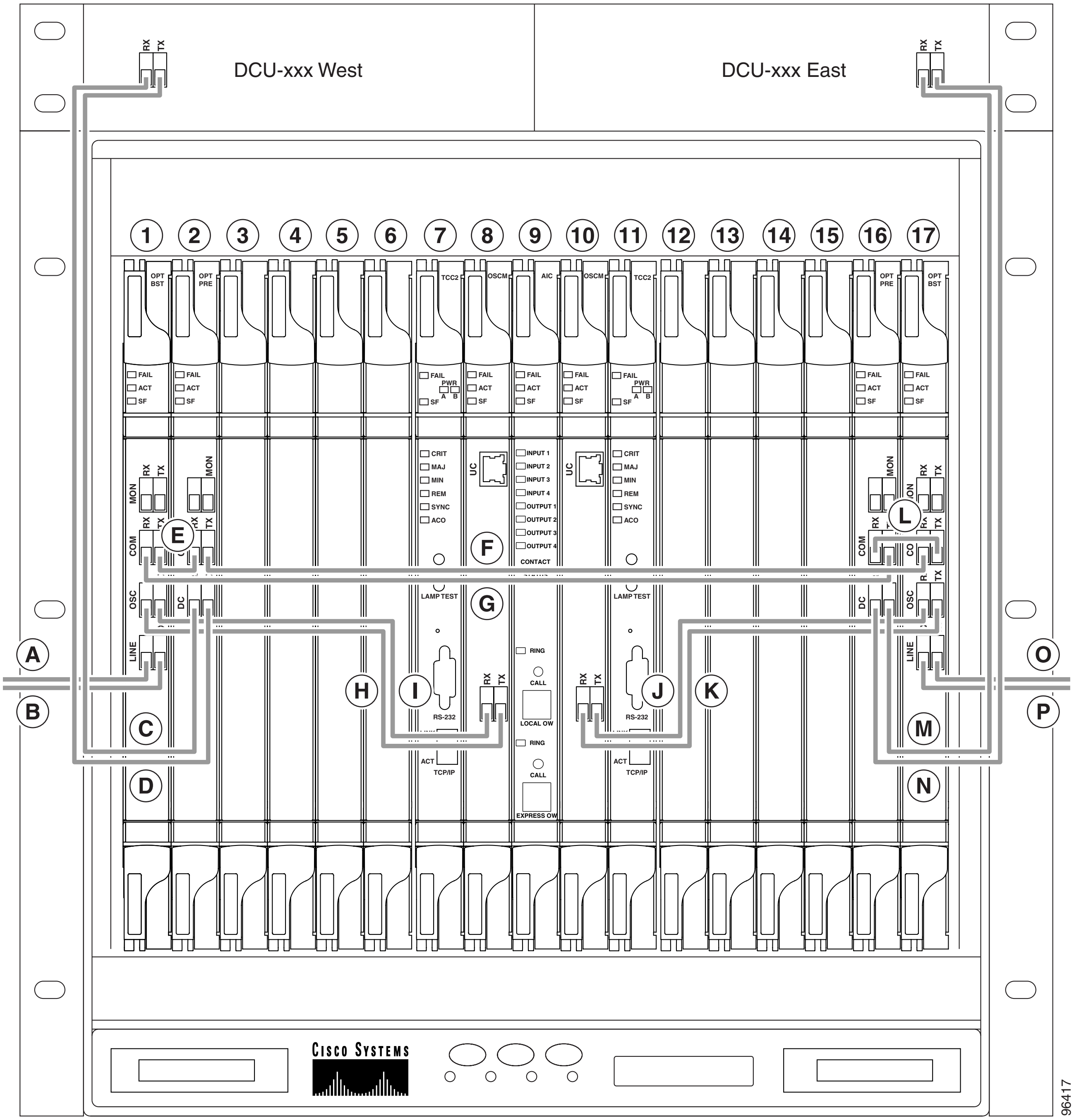
Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Refer to your site plan when cabling the node. Connect fiber-optic cabling for the line amplifier node by consulting the following rules:

- Line amplifier node layout allows all combinations of OPT-PRE and OPT-BST and allows you to use asymmetrical card choices in west-to-east and east-to-west configurations. For a given line direction, you can configure the four following possibilities:
  - Only preamplification
  - Only booster amplification
  - Both pre- and booster amplification (where a line amplifier node has amplification in at least one direction)
  - Neither pre- nor booster amplification
- If an OPT-PRE card is present west-to-east:
  - The West OSC-CSM or OPT-BST COM Tx is connected to the West OPT-PRE COM Rx port
  - The West OPT-PRE COM Tx port is connected to the East OSC-CSM or OPT-BST COM Rx port
- If an OPT-PRE card is not present west-to-east, the West OSC-CSM or the OPT-BST COM Tx port is connected to the East OSC-CSM or OPT-BST COM Rx port.
- If an OPT-PRE card is present east-to-west:
  - The East OSC-CSM or OPT-BST COM Tx port is connected to the East OPT-PRE COM Rx port.
  - The East OPT-PRE COM Tx port is connected to the West OSC-CSM or OPT-BST COM Rx port.
- If an OPT-PRE card is not present east-to-west, the East OSC-CSM or OPT-BST COM Tx port is connected to the West OSC-CSM or OPT-BST COM Rx port.

Figure 2-9 shows a sample line amplifier node with cabling.

Figure 2-9 Fibering a Line Amplifier Node



1	Slot 1OPT-BST West	**A**	Slot 1 Line Rx from span fiber
2	Slot 2 OPT-PRE West	**B**	Slot 1 Line Tx to span fiber
3	Slot 3 (not required for configuration)	**C**	DCU West Tx to Slot 2 DC Rx
4	Slot 4 (not required for configuration)	**D**	DCU West Rx from Slot 2 DC Tx
5	Slot 5 (not required for configuration)	**E**	Slot 1 COM Tx to Slot 2COM Rx

6	Slot 6 (not required for configuration)	**F**	Slot 2 COM Tx to Slot 17 COM Rx
7	Slot 7 TCC2	**G**	Slot 1 COM Rx from Slot 16 COM Tx
8	Slot 8 OSCM West	**H**	Slot 1 OSC Rx from Slot 8 Tx
9	Slot 9 AIC	**I**	Slot 1 OSC Tx to Slot 8 Rx
10	Slot 10 OSCM East	**J**	Slot 10 Tx to Slot 17 OSC Rx
11	Slot 11 TCC2	**K**	Slot 10 Rx from Slot 17 OSC Tx
12	Slot 12 (not required for configuration)	**L**	Slot 16 COM Rx from Slot 17 COM Tx
13	Slot 13 (not required for configuration)	**M**	Slot 16 DC Tx to DCU-East Rx
14	Slot 14 (not required for configuration)	**N**	Slot 16 DC Rx from DCU-East Tx
15	Slot 15 (not required for configuration)	**O**	Slot 17 Line Tx to span fiber
16	Slot 16 OPT-PRE East	**P**	Slot 17 Line Rx from span fiber
17	Slot 17 OPT-BST East	**—**	

Step 2 Plug one end of the fiber cable into the desired Rx port and other end into the desired Tx port.

Note The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat Step 2 until you have connected the nodes according to the site plan.

Step 4 Return to your originating procedure (NTP).

DLP-A427 Install Fiber-Optic Cables for an Amplified or Passive OADM Node

Purpose	This task gives instructions, rules, and examples to install fiber-optic cables on an amplified or passive optical add/drop multiplexing (OADM) node in a DWDM shelf. See Chapter 7, "Turn Up DWDM Network" to provision and test DWDM configurations.
Tools	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 17-21
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Amplified OADM nodes contain OPT-PRE cards and/or OPT-BST cards. Passive OADM nodes do not. Both contain add/drop channel or band cards or 32MUX-O and 32DMX-O cards.

Note To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Step 1 Refer to your site plan when cabling the node. Connect fiber-optic cabling for amplified or passive OADM nodes by consulting the following rules:

- The two sides of the OADM node do not need to be symmetrical. On each side, you can create one of the following four configurations:
  - OPT-BST and OPT-PRE
  - OSC-CSM and OPT-PRE
  - Only OSC-CSM
  - Only OPT-BST
- Regardless of direction, the TCC2 card supervision always assumes the AD-xC or AD-xB COM Rx port and COM Tx ports are connected.

Step 2 Consult the following rules for OADM node express path cabled connections:

- The TCC2 card checks and guarantees that the AD-xB or AD-xC port sequence on the west line side is the same as the AD-xC or AD-xB port sequence on the East side.
- Regardless of direction, the TCC2 card supervision always assumes that the AD-xC or AD-xB EXP-Rx and EXP-Tx port are connected.
- When you set a connection between an AD-xC or AD-xB 1 EXP Tx port and an AD-xC or AD-xB 2 COM Rx port, the TCC2 card automatically assumes the same connection between the other AD-xC or AD-xB 1 EXP Rx port and AD-xC or AD-xC 2 COM Tx port.
- Tx ports should only be connected to Rx ports.
- EXP ports are connected only to COM ports in between AD-xC or AD-xB cards that all belong to the east side (that is, they are daisy-chained).
- EXP ports are connected only to COM ports in between AD-xC or AD-xB cards that belong to the West side.
- The EXP port of the last AD-xC or AD-xB card in the west side is connected to the EXP port of the first AD-xC or AD-xB card in the east side.
- The OPT-BST COM Rx port is connected to the nearest (in slot position) AD-xC or AD-xB COM Tx port.
- The OPT-PRE COM Tx port is connected to the nearest (in slot position) AD-xC or AD-xB COM Rx port.
- If OADM cards are located in adjacent slots, the TCC2 card assumes they are connected in a daisy-chain between the EXP ports and COM ports as noted above.
- The first west AD-xC or AD-xB card COM Rx port is connected to the west OPT-PRE or OSC-CSM COM Tx port.
- The first west AD-xC or AD-xB card COM Tx port is connected to the west OPT-BST or OSC-CSM COM Rx port.
- The first east AD-xC or AD-xB card COM Rx port is connected to the east OPT-PRE or OSC-CSM COM Tx port.

- The first east AD-xC or AD-xB COM Tx port is connected to the east OPT-BST or OSC-CSM Rx port.
- If a west OPT-PRE is present, the west OPT-BST or OSC-CSM COM Tx port is connected to the west OPT-PRE COM Rx port.
- If an east OPT-PRE is present, the east OPT-BST or OSC-CSM COM Tx port is connected to the east OPT-PRE COM Rx port.

Step 3 Consult the following rules for OADM node add/drop path cabled connections:

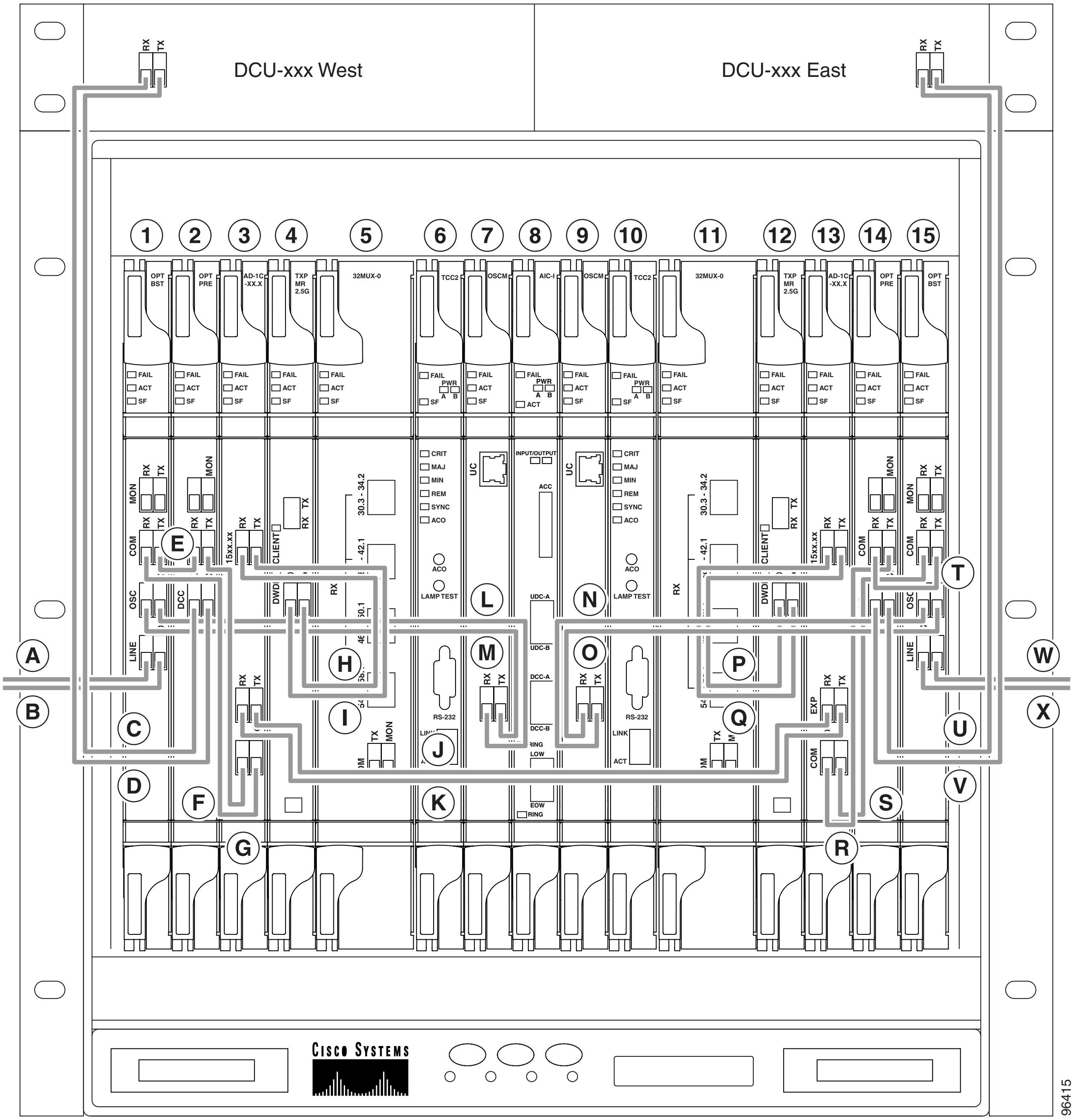
- AD-xB add/drop (Rx or Tx) ports are only connected to the following ports:
  - 4MD COM Tx or 4MD COM Rx ports
  - another AD-xB add/drop port (a pass-through configuration)
- An AD-xB add/drop band port is only connected to a 4MD card belonging to the same band.
- For each specific AD-xB, the add and drop ports for that band card are connected to the COM Tx and COM Rx ports of the same 4MD card.
- The AD-xB and 4MD card are located in the same direction side (the connected ports will all have the same line direction).

Step 4 Consult the following rules for OADM node pass-through path cabled connections:

- Pass-through connections are only established between add and drop ports on the same band or channel and same line direction.
- Only connect AD-xC or AD-xB channel add/drop ports to other AD-xC or AD-xB add/drop ports (as pass-through configurations).
- An add (Rx) port is only connected to a drop (Tx) port.
- Only connect 4MD client input/output ports to other 4MD client input/output ports.
- Only connect a 32DMX-O output port to a 32MUX-O input port.
- A West AD-xB drop (Tx) port is connected to the corresponding west 4MD COM Rx port.
- A West AD-xB add (Rx) port is connected to the corresponding west 4MD COM Tx port.
- An East AD-xB drop (Tx) port is connected to the corresponding east 4MD COM Rx port.
- An East AD-xB add (Rx) port is connected to the corresponding east 4MD COM Tx port.

Figure 2-10 shows a sample amplified OADM node with cabling.

Figure 2-10 Fibering an Amplified OADM Node

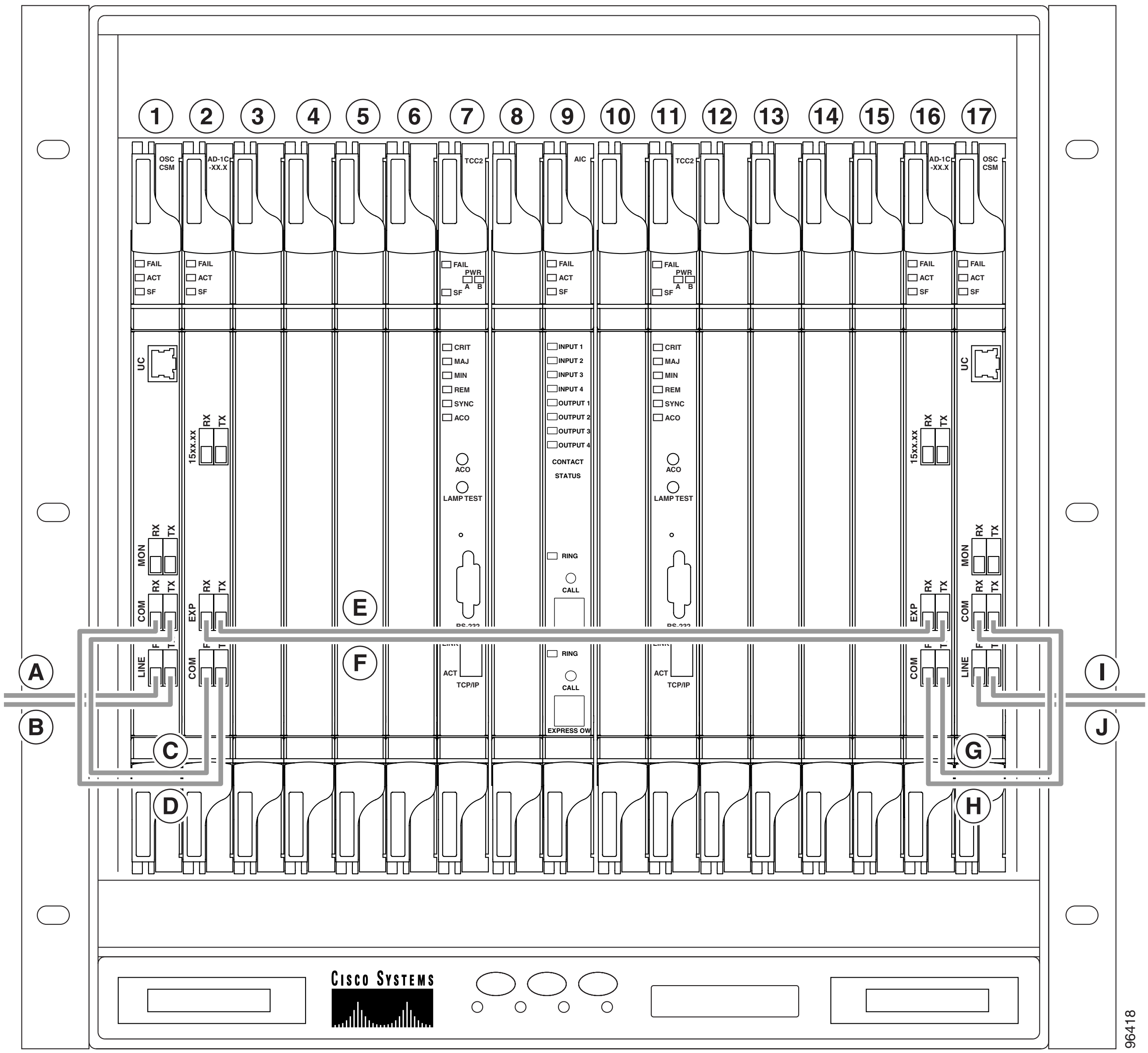


1	Slot 1 OPT-BST West	**F**	Slot 1 COM Rx from Slot 3 COM Tx
2	Slot 2 OPT-PRE West	**G**	Slot 2 COM Tx to Slot 3 COM Rx
3	Slot 3 AD-1C-xx.x (OADM card) West	**H**	Slot 3 channel Rx from Slot 4 DWDM Tx
4	Slot 4 TxP_MR_2.5G (Transponder) West	**I**	Slot 3 channel Tx to Slot 4 DWDM Rx
5	Slot 5-6 32MUX-O West	**J**	Slot 3 EXP Tx to Slot 15 EXP Rx

6	Slot 7 TCC2	**K**	Slot 3 EXP Rx from Slot 15 EXP Tx
7	Slot 8 OSCM West	**L**	Slot 1 OSC Tx to Slot 8 Rx
8	Slot 9 AIC-I	**M**	Slot 1 OSC Rx from Slot 8 Tx
9	Slot 10 OSCM East	**N**	Slot 10 Rx from Slot 17 OSC Tx
10	Slot 11 TCC2	**O**	Slot 10 Tx to Slot 17 OSC Rx
11	Slot 12-13 32MUX-O East	**P**	Slot 14 DWDM Rx from Slot 15 Channel Tx
12	Slot 14 TxP_MR_2.5G (Transponder) East	**Q**	Slot 14 DWDM Tx to Slot 15 Channel Rx
13	Slot 15 AD-1C-xx.x (OADM card) East	**R**	Slot 15 COM Rx from Slot 16 COM Tx
14	Slot 16 OPT-PRE East	**S**	Slot 15 COM Tx to Slot 17 COM Rx
15	Slot 17 OPT-BST East	**T**	Slot 16 COM Rx from Slot 17 COM Tx
A	Slot 1 Line Rx from span fiber	**U**	Slot 16 DC Tx to DCU-East Rx
B	Slot 1 Line Tx to span fiber	**V**	Slot 16 DC Rx from DCU-East Tx
C	DCU West Tx to Slot 2 DC Rx	**W**	Slot 17 Line Tx to span fiber
D	DCU West Rx from Slot 2 DC Tx	**X**	Slot 17 Line Rx from span fiber
E	Slot 1 COM Tx to Slot 2 COM Rx	**—**	

Figure 2-11 shows an example of a passive OADM node.

Figure 2-11 Fibering a Passive OADM Node



1	Slot 1 OSC-CSM West	**15**	Slot 15 (not necessary for configuration)
2	Slot 2 AD-1C-xx.x (OADM) West	**16**	Slot 16 AD-1C-xx.x (OADM) West
3	Slot 3 (not necessary for configuration)	**17**	Slot 17 OSC-CSM East
4	Slot 4 (not necessary for configuration)	**A**	Slot 1 Line Rx from span fiber
5	Slot 5 (not necessary for configuration)	**B**	Slot 1 Line Tx to span fiber
6	Slot 6 (not necessary for configuration)	**C**	Slot 1 COM Tx to Slot 2 COM Rx
7	Slot 7 TCC2	**D**	Slot 1 COM Rx from Slot 2 COM Tx
8	Slot 7 TCC2	**E**	Slot 2 EXP Tx to Slot 16 EXP Rx

9	Slot 9 AIC	**F**	Slot 2 EXP Rx from Slot 16 EXP Tx
10	Slot 10 (not necessary for configuration	**G**	Slot 16 COM Tx to Slot 17 COM Rx
11	Slot 11 TCC2	**H**	Slot 16 COM Rx from Slot 17 COM Tx
12	Slot 12 (not necessary for configuration	**I**	Slot 17 Line Tx to span fiber
13	Slot 13 (not necessary for configuration)	**J**	Slot 17 Line Rx from span fiber
14	Slot 14 (not necessary for configuration)	—	

Step 5 Plug one end of the fiber cable into the desired Rx port and other end into the desired Tx port.

Note The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 6 Repeat Step 5 until you have connected the nodes according to the site plan.

Step 7 Return to your originating procedure (NTP).

NTP-A245 Route Fiber-Optic Cables

Purpose	This procedure describes how to route fiber-optic cables. This procedure can be used for TDM, DWDM, and hybrid nodes.
Tools/Equipment	None
Prerequisite Procedures	Any of the following: NTP-A247 Install Fiber-Optic Cables on OC-N Cards, page 2-29 NTP-A244 Install Fiber-Optic Cables on DWDM Cards, page 2-41 NTP-A274 Install the FC_MR-4 Cards, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the fold-down front door on the cable-management tray.

Step 2 Route the fiber cable on the card faceplate through the fiber clip on the faceplate, if provided. Fiber clips are factory-attached to the faceplate of OC-N card and to some DWDM cards (32MUX-O, 32DMX-O, OSCM, OPT-PRE, and OPT-BST).

GBICs do not have fiber clips; therefore, if you are routing fiber from an E1000-2-G, E1000-2, G1000-2-G, G10002, or FC_MR-4 card, skip to Step 3.

Step 3 Route the fiber cables into the cable-management tray.

Step 4 Route the fiber cables out either side of the cable-management tray through the cutouts on each side of the shelf assembly. Use the reversible fiber guides to route cables out the desired side.

Step 5 Close the fold-down front door when all fiber cables in the front compartment are properly routed.

Stop. You have completed this procedure.

NTP-A116 Remove and Replace a Card

Purpose	This procedure removes and replaces all cards housed in the ONS 15454 shelf and rack.
Tools/Equipment	None
Prerequisite Procedures	A card installation procedure
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are not logged into CTC and you need to remove a card, remove the card as described in Step 3. When you log into CTC, troubleshoot the mismatched equipment alarm (MEA) with the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 If you are logged into CTC, complete one of the following:

- Complete the "DLP-A191 Delete a Card" task on page 2-58 and continue with Step 3.
- Complete the "DLP-A247 Change an OC-N Card" task on page 2-58 to delete a card and replace it with a different OC-N card while maintaining existing provisioning.

Step 3 Physically remove the card:

a. Open the card latches/ejectors.

b. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 4 Insert the new card using one of the following procedures as applicable:

- NTP-A15 Install the Common Control Cards, page 2-2
- NTP-A16 Install the OC-N Cards, page 2-12
- NTP-A249 Install the Transponder and Muxponder Cards, page 2-14
- NTP-A17 Install the Electrical Cards, page 2-16
- NTP-A246 Install Ethernet Cards and Connectors, page 2-17
- NTP-A274 Install the FC_MR-4 Cards, page 2-23
- NTP-A242 Install the DWDM Cards, page 2-25
- NTP-A243 Install the DWDM Dispersion Compensating Cards, page 2-28

Step 5 Continue with the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29 or the "NTP-A244 Install Fiber-Optic Cables on DWDM Cards" procedure on page 2-41

Stop. You have completed this procedure.

DLP-A191 Delete a Card

Purpose	This task deletes a card from CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the shelf graphic in CTC, right-click the card that you want to remove and choose **Delete Card**.

You cannot delete a card if any of the following conditions apply:

- The card is a TCC2 card. To replace a TCC2 card, refer to the *Cisco ONS 15454 Troubleshooting Guide*.
- The card is part of a protection group; see the "DLP-A155 Delete a Protection Group" task on page 12-20.
- The card has circuits; see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19 and the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18.
- The card is part of a BLSR; see the "NTP-A213 Remove a BLSR Node" procedure on page 16-9.
- The card is being used for timing; see the "DLP-A157 Change the Node Timing Source" task on page 12-23.
- The card has a non-DWDM DCC/GCC termination; see the "NTP-A255 Delete Communications Channel Terminations" procedure on page 12-20.

Note If you delete a card in CTC but do not remove it from the shelf, it will reboot and reappear in CTC.

Step 2 Return to your originating procedure (NTP).

DLP-A247 Change an OC-N Card

Purpose	This task changes an OC-N card while maintaining existing provisioning, including DCCs/GCCs, circuits, protection, timing, and rings. This task is intended to be used when a slot is preprovisioned and you want to change the optical speed of the card, or when you have backed out of an automatic span upgrade.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Physically removing an OC-N card can cause a loss of working traffic or a protection switch. See Chapter 14, "Upgrade Cards and Spans" for information on upgrading traffic to a higher speed.

Note You cannot change a multiport card to a card with a smaller number of ports.

Step 1 If the card the active card in a 1+1 protection group, switch traffic away from the card:

a. Log into a node on the network. If you are already logged in, go to Step b.

b. Display the CTC node (login) view.

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

d. Double-click the protection group that contains the reporting card.

e. Click the active card of the selected group.

f. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 2 In CTC, right-click the card that you want to remove and choose **Change Card**.

Step 3 From the Change Card drop-down menu, choose the desired card type and click **OK**. An MEA alarm appears until you replace the card.

Step 4 Physically remove the card:

a. Disconnect any fiber connections to the front of the card.

b. Open the card latches/ejectors.

c. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 5 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12.

Step 6 Return to your originating procedure (NTP).

NTP-A20 Replace the Front Door

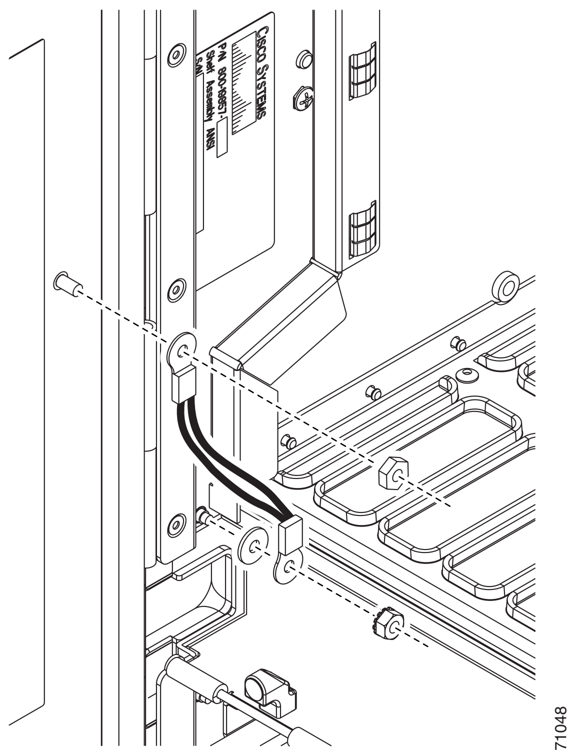
Purpose	This procedure replaces the front door and door ground strap after installing cards and fiber-optic cables.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-A3 Open and Remove the Front Door, page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note Be careful not to crimp any fiber cables that are connected to the OC-N cards or DWDM cards. Some might not have the fiber boot attached.

Step 1 Insert the front door into the hinges on the shelf assembly.

Step 2 Attach one end of the ground strap terminal lug (72-3622-01) to the male stud on the inside of the door. Attach and tighten the #6 Kepnut (49-0600-01) using the open-end wrench (Figure 2-12).

Figure 2-12 Installing the Door Ground Strap Retrofit Kit



Step 3 Attach the other end of the ground strap to the longer screw on the fiber guide.

a. Attach the lock washer.

b. Attach the terminal lug.

c. Using the open-end wrench, attach and tighten the #4 Kepnut (49-0337-01) on the terminal lug.

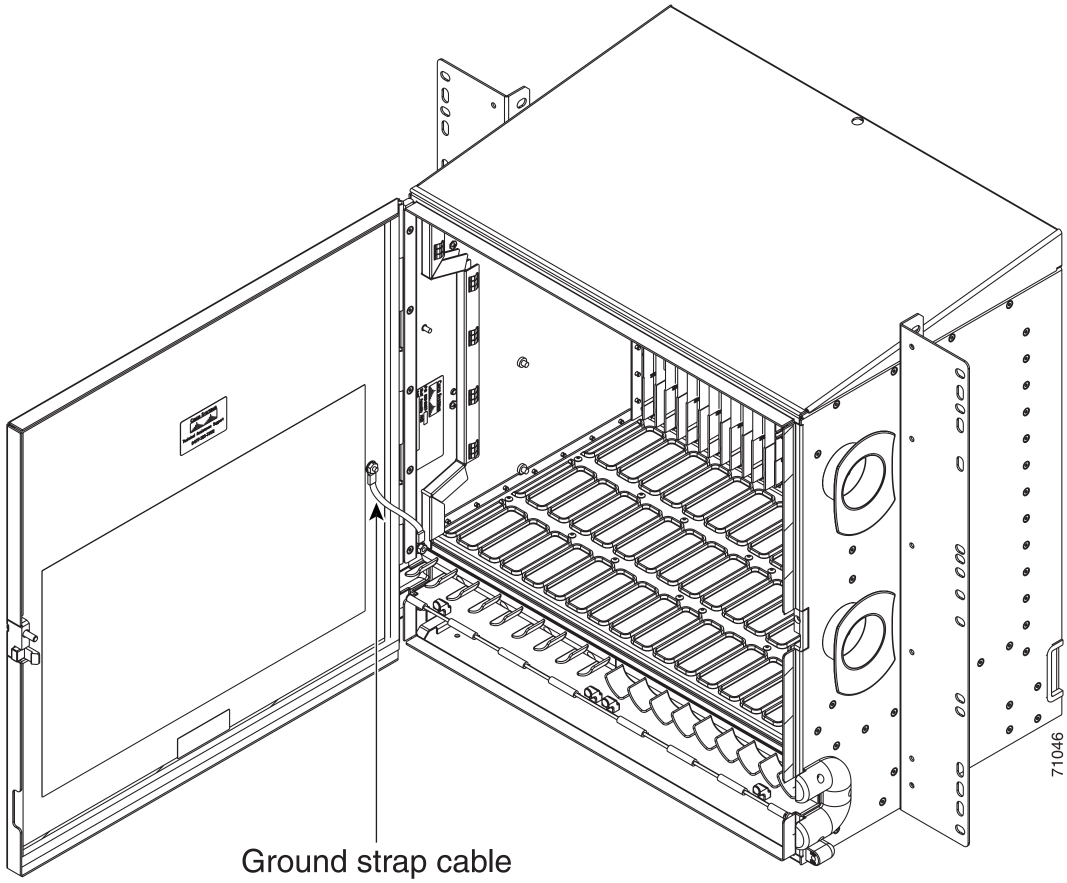
> **Note** To avoid interference with the traffic (line) card, make sure the ground strap is in a flat position when the door is open. To move the ground strap into a flat position, rotate the terminal lug counterclockwise before tightening the Kepnut.

Step 4 Replace the left cable-routing channel.

Step 5 Using a Phillips screwdriver, insert and tighten the screws for the cable-routing channel.

Figure 2-13 shows the shelf assembly with the front door and ground strap installed.

Figure 2-13 Shelf Assembly with Door Ground Strap Retrofit Kit Installed



Step 6 Swing the door closed.

Note The ONS 15454 comes with a pinned hex key tool for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

Stop. You have completed this procedure.

Connect the PC and Log into the GUI

This chapter explains how to connect PCs and workstations to the Cisco ONS 15454 and how to log into Cisco Transport Controller (CTC) software, which is the ONS 15454 Operation, Administration, Maintenance and Provisioning (OAM&P) user interface. Procedures for connecting to the ONS 15454 using TL1 are provided in the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A260 Set Up Computer for CTC, page 3-1—Complete this procedure if your PC or workstation has never been connected to an ONS 15454.
2. NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-8—Complete this procedure to set up your computer for an onsite craft connection to the ONS 15454.
3. NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-19—Complete this procedure to set up your computer to connect to the ONS 15454 using a corporate LAN.
4. NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-21—Complete this procedure to set up your computer for remote modem access to the ONS 15454.
5. NTP-A23 Log into the ONS 15454 GUI, page 3-22—Complete this procedure to log into CTC.

NTP-A260 Set Up Computer for CTC

Purpose	This procedure configures your PC or UNIX workstation to run CTC.
Tools/Equipment	Cisco ONS 15454 Release 4.6 software or documentation CD
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer does not have an appropriate browser installed, complete the following:

- To install Netscape 4.76 or 7.x, download the browser at the following site: http://channels.netscape.com/ns/browsers/default.jsp
- To install Internet Explorer 6.x on a PC, download the browser at the following site: http://www.microsoft.com

Step 2 If your computer is a Windows PC, complete the "DLP-A337 Run the CTC Installation Wizard for Windows" task on page 3-2, then go to Step 4.

Step 3 If your computer is a UNIX workstation, complete the "DLP-A338 Run the CTC Installation Wizard for UNIX" task on page 3-5.

Step 4 When your PC or workstation is set up, continue with the setup procedure appropriate to your network:

- NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-8
- NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-19
- NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-21

Stop. You have completed this procedure.

DLP-A337 Run the CTC Installation Wizard for Windows

Purpose	This task installs CTC online help and JRE 1.4.2, as necessary. JRE 1.3.1_02 or JRE 1.4.2 are required to run CTC on Windows. Cisco recommends using JRE 1.4.2 with Netscape 7.x.
Tools/Equipment	Cisco ONS 15454 Release 4.6 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • JRE 1.3.1_02 or JRE 1.4.2 are not installed • CTC online help is not installed and is needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Verify that your computer has the following:

- Processor—Pentium III, 700 Mhz or faster
- RAM—256 MB
- Hard drive—50 MB of space must be available
- Operating System—Windows 98, Windows NT 4.0, Windows 2000, or Windows XP

  If your operating system is Windows NT 4.0, verify that Service Pack 5 or later is installed. From the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 5 or later is not installed, do not continue. Install Service Pack 5 following the computer upgrade procedures for your site.

> **Note** Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15454 Reference Manual* for computer requirements needed for small, medium, and large ONS 15454 networks.

Step 2 Insert the Cisco ONS 15454 Release 4.6 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Online Help

Step 3 Click **Next**.

Step 4 Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and Online Help. If you already have JRE 1.4.2 installed on your computer, choose Custom.
- Click **Custom** if you want to install either the JRE or the Online Help.

> **Note** Choose Custom and do not install JRE 1.4.2 if you must launch CTC from nodes running a release earlier than R4.6, or you have web applications that are sensitive to JRE changes.

Step 5 Click **Next**.

Step 6 Complete the following, as applicable:

- If you selected Typical, skip this step and continue with Step 7.
- If you selected Custom in Step 4, check the CTC component that you want to install and click **Next**.
  - If you selected Online Help, continue with Step 7.
  - If you did not select Online Help, continue with Step 9.

Step 7 The directory where the installation wizard will install CTC online help appears. The default is C:\Program Files\Cisco\CTC\Documentation.

- If you want to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the directory, skip this step.

Step 8 Click **Next**.

Step 9 Review the components that will be installed. If you want to change the components, complete one of the following:

- If you selected Typical in Step 4, click **Back** twice to return to the installation setup type panel. Choose **Custom** and repeat Steps 5 through 8.
- If you selected Custom in Step 4, click **Back once or twice (depending on the components selected) until the component selection panel appears.** Repeat Steps 6 through 8.

Step 10 Click **Next**. It may take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 and did not check Java Runtime Environment 1.4.2, continue with Step 12.

Step 11 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step b.
- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 12.

Note If JRE 1.4.2 is already installed on your computer, the License Agreement panel does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down menu for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.4.2 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down menu options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don’t install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE as the default for these browsers may cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

> **Note** If you are uninstalling the JRE, click Remove.

Step 12 In the Cisco Transport Controller Installation Wizard, click **Next**. The Online Help installs.

Step 13 Click **Finish**.

Step 14 Return to your originating procedure (NTP).

DLP-A338 Run the CTC Installation Wizard for UNIX

Purpose	This task installs CTC online help and JRE 1.4.2, as necessary. JRE 1.3.1_02 (Netscape 4.76) or JRE 1.4.2 (Netscape 7.x) are required to run CTC.
Tools/Equipment	Cisco ONS 15454 Release 4.6 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • JRE 1.3.1_02 or 1.4.2 are not installed. • CTC online help is not installed and is needed.
Onsite/Remote	Onsite or remote
Security Level	None

> **Note** Cisco does not recommend upgrading to JRE 1.4.2 if CTC must be launched directly from nodes running software earlier than Release 4.6. If you upgrade to JRE 1.4.2, you must use Netscape 7.x.

Step 1 Verify that your computer has the following:

- RAM—256 MB
- Hard drive—50 MB of space must be available
- Operating System—Solaris 8 and 9

> **Note** These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15454 Reference Manual* for computer requirements needed for small, medium, and large ONS 15454 networks.

Step 2 Change the directory, type:

`cd /cdrom/cdrom0/`

Step 3 From the techdoc454 CD directory, type:

`./setup.bat`

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Online Help

Step 4 Click **Next**.

Step 5 Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and Online Help. If you already have JRE 1.4.2 installed on your computer, choose Custom.
- Click **Custom** if you want to install either the JRE or the Online Help.

Note Choose Custom and do not install JRE 1.4.2 if you must launch CTC from nodes running a release earlier than R4.6, or you have web applications that are sensitive to JRE changes.

Step 6 Click **Next**.

Step 7 Complete the following, as applicable:

- If you selected Typical, continue with Step 8.
- If you selected Custom in Step 5, check the CTC component that you want to install and click **Next**.
  - If you selected Online Help, continue with Step 8.
  - If you did not select Online Help, continue with Step 10.

Step 8 The directory where the installation wizard will install CTC online help appears. The default is /usr/doc/ctc.

- If you want to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the CTC online help directory, skip this step.

Step 9 Click **Next**.

Step 10 Review the components that will be installed.

- If you selected Typical in Step 5, click **Back** twice to return to the installation setup type panel. Choose **Custom** and repeat Steps 6 through 9.
- If you selected Custom in Step 5, click **Back once or twice (depending on the components selected) you reach the component selection panel and check the desired components**. Repeat Steps 7 through 9.

Step 11 Click **Next**. It may take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 and did not check Java Runtime Environment 1.4.2, continue with Step 13.

Step 12 To install the JRE, complete the following:

a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step b.
- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13.

Note If JRE 1.4.2 is already installed on your computer, the License Agreement panel does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down menu for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 1.4.2 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down menu options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

f. Click **Next**.

g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

Note Setting the JRE version as the default for these browsers may cause problems with these browsers.

h. Click **Next**.

i. Click **Finish**.

Note If you are uninstalling the JRE, click Remove.

Step 13 In the Cisco Transport Controller Installation Wizard, click **Next**. The Online Help installs.

Step 14 Click **Finish**.

Note Be sure to record the names of the directories you choose for JRE and the online help.

Step 15 Return to your originating procedure (NTP).

NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454

Purpose	This procedure explains how to set up a PC running Windows or a Solaris workstation for an onsite local craft connection to the ONS 15454.
Tools/Equipment	Depends on connection type
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Complete one of the CTC computer setup tasks shown in Table 3-1 based your CTC connection environment.

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15454

CTC Connection Environment	CTC Computer Setup Task
• You are connecting from a Windows PC. • All nodes that you will access run software earlier than Release 3.3. • You will connect to one ONS 15454. • You need to access non-ONS 15454 applications such as ping and tracert.	DLP-A50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses, page 3-9
• You are connecting from a Windows PC. • The CTC computer is provisioned for Dynamic Host Configuration Protocol (DHCP). • The ONS 15454 has DHCP forwarding enabled. • The ONS 15454 is connected to a DHCP server. **Note** The ONS 15454 does not provide IP addresses. If DHCP is enabled, it passes DCHP requests to an external DHCP server.	DLP-A51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Dynamic Host Configuration Protocol, page 3-12 **Note** Do not use this task for initial node turnup. Use the task only if DHCP forwarding is enabled on the ONS 15454. By default, DHCP is not enabled. To enable it, see the "NTP-A169 Set Up CTC Network Access" procedure on page 4-9.

Table 3-1 CTC Computer Setup for Local Craft Connections to the ONS 15454 (continued)

CTC Connection Environment	CTC Computer Setup Task
• You are connecting from a Windows PC. • All nodes that you will access run software Release 3.3 or later. • You will connect to ONS 15454s at different locations and times and do not wish to reconfigure your PC's IP settings each time. • You will not access or use non-ONS 15454 applications such as ping and tracert. • You will connect to the ONS 15454 TCC2 Ethernet port or backplane LAN pins either directly or through a hub.	DLP-A52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection, page 3-14
• You are connecting from a Solaris Workstation. • You will connect to one ONS 15454. • You need to access non-ONS 15454 applications such as ping and traceroute.	DLP-A53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454, page 3-17

Step 2 After setting up your CTC computer, continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-22, if applicable.

Stop. You have completed this procedure.

DLP-A50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15454 when: • You will access nodes running software releases earlier than Software Release 3.3. • You will connect to one ONS 15454; if you will connect to multiple ONS 15454s, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15454. • You need to use non-ONS 15454 applications such as ping and trace route.
Tools/Equipment	Network interface card (NIC), also referred to as an Ethernet card
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the ONS 15454 IP address. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address shown on the ONS 15454 LCD except for the last octet. The last octet must be 1 or 3 through 254.

g. In the Subnet Mask field, type **255.255.255.0**.

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the ONS 15454 IP address in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. In some cases, Windows NT 4.0 prompts you to reboot your PC. If you receive this prompt, click **Yes**.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address shown on the ONS 15454 LCD except for the last octet. The last octet must be 1 or 3 through 254.

f. In the Subnet Mask field, type **255.255.255.0**.

g. In the Default Gateway field, type the ONS 15454 IP address.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections**.

> **Note** If the Network Connections menu is not available, click **Switch to Classic View**.

b. From the Network Connections dialog box, click the **Local Area Connection** icon.

c. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address shown on the ONS 15454 LCD except for the last octet. The last octet must be 1 or 3 through 254.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15454 IP address.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Dynamic Host Configuration Protocol

Purpose	This task sets up your computer for craft connection to the ONS 15454 using DHCP.
Tools/Equipment	Straight-through (Category 5) LAN cable
	NIC
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
	NTP-A169 Set Up CTC Network Access, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Do not use this task for initial node turnup. Use the task only if DHCP forwarding is enabled on the ONS 15454. By default, DHCP is not enabled. To enable it, see the "NTP-A169 Set Up CTC Network Access" procedure on page 4-9.

Note The ONS 15454 does not provide the IP addresses. If DHCP forwarding is enabled, it passes DCHP requests to an external DHCP server.

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your NIC, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Obtain an IP address automatically**.

h. Click **OK**.

i. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. Click **Apply**.

h. If Windows prompts you to restart your PC, click **Yes**.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Obtain an IP address from a DHCP server**.

e. Click **OK**.

f. In the Local Area Connection Properties dialog box, click **OK**.

g. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections.**

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. In the Network Connections dialog box, click **Local Area Connection**.

c. In the Local Area Connection Status dialog box, click **Properties**.

d. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

e. Click **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. In the Local Area Connection Properties dialog box, click **OK**.

h. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15454 when: • You will connect to the ONS 15454 Ethernet port or backplane LAN pins either directly or through a hub. • All nodes that you will access are running Software Release 3.3 or later. • You will connect to multiple ONS 15454s and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15454 applications such as ping and tracert.
Tools/Equipment	NIC
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

> **Note** In Windows XP, you can select Control Panel directly from the Start menu. Make sure you are in Classic View before continuing with this procedure.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP.

Step 2 According to the Windows operating system installed on your computer, perform one of the following steps:

- For Windows 98, complete Step 3.
- For Windows NT 4.0, complete Step 4.
- For Windows 2000, complete Step 5.
- For Windows XP, complete Step 6.

Step 3 If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your NIC, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.

> **Note** You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 12-5.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the address entered in Step h. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 4 If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.

> **Note** You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 12-5.

g. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the IP address entered in Step f in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. Reboot your PC.

Step 5 If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.

Note You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 12-5.

f. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

g. Type the IP address entered in Step e in the Gateway Address field.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 6 If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

a. From the Windows Start menu, choose **Control Panel > Network Connections**.

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. From the Network Connections dialog box, click the **Local Area Connection** icon.

c. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.

Note You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 12-5.

e. In the Subnet Mask field, type the same subnet mask as the ONS 15454. The default is **255.255.255.0** (24 bit).

f. Type the IP address entered in Step d in the Gateway Address field.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Log into the workstation as the root user.

Step 2 Check to see if the interface is plumbed by typing:

 # ifconfig ***device*** (For example, # **ifconfig hme1**)

If the interface is plumbed, a message similar to the following appears:

```
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask
0
```

If a message similar to this one appears, go to Step 4.

If the interface is not plumbed, a message similar to the following appears:

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

If a message similar to this one appears, go to Step 3.

Step 3 Plumb the interface by typing:

 # ifconfig ***device*** **plumb**

For example:

ifconfig hme1 plumb

Step 4 Configure the IP address on the interface by typing:

 # ifconfig ***interface ip-address*** **netmask** ***netmask*** **up**

For example:

ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up

Note Enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254.

Step 5 In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Craft Access Only on the Provisioning > Network > General > Gateway Settings tab.

Step 6 Test the connection:

a. Start Netscape Navigator.

b. Enter the ONS 15454 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the "DLP-A60 Log into CTC" task on page 3-24 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

ping ***ONS-15454-IP-address***

For example, to connect to an ONS 15454 with a default IP address of 192.1.0.2, type:

ping 192.1.0.2

If your workstation is connected to the ONS 15454, the following message appears:

IP-address is alive

> **Note** Skip this step if you checked the Craft Access Only check box at Provisioning > Network > General > Gateway Settings.

d. If CTC is not responding, a "Request timed out" (Windows) or a "no answer fromx.x.x.x" (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15454 are securely attached. Check the link status by typing:

```
# ndd -set /dev/device instance 0
# ndd -get /dev/device link_status
```

For example:

```
# ndd -set /dev/hme instance 0
# ndd -get /dev/hme link_status
```

A result of "1" means the link is up. A result of "0" means the link is down.

> **Note** Check the man page for ndd. For example: # **man ndd**.

Step 7 Return to your originating procedure (NTP).

NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454

Purpose	This procedure sets up your computer to access the ONS 15454 through a corporate LAN. To complete this procedure: • The ONS 15454 must be provisioned for LAN connectivity, including IP address, subnet mask, default gateway. • The ONS 15454 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is already connected to the corporate LAN, go to Step 2. If you changed your computer's network settings for craft access to the ONS 15454, change the settings back to the corporate LAN access settings. This generally means:

- Set the IP Address on the TCP/IP dialog box back to **Obtain an IP address automatically** (Windows 98) or **Obtain an IP address from a DHCP server** (Windows NT 4.0, 2000, or XP).
- If your LAN requires that DNS or WINS be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 2 If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 nodes as exceptions. To disable proxy service, complete one of the following tasks, depending on the web browser that you use:

- DLP-A56 Disable Proxy Service Using Internet Explorer (Windows), page 3-20
- DLP-A57 Disable Proxy Service Using Netscape (Windows and UNIX), page 3-20

Step 3 Continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-22.

Stop. You have completed this procedure.

DLP-A56 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer. Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From the Start menu, select **Settings > Control Panel**.

> **Note** If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 In the Internet Properties dialog box, click **Connections** > **LAN Settings**.

Step 4 In the LAN Settings dialog box, complete one of the following tasks:

- Uncheck **Use a proxy server** to disable the service.
- Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15454 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS 15454s on your network. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-A57 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape. It is required if your computer is connected to a network computer proxy server and your browser is Netscape.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Open Netscape.

Step 2 From the Edit menu, choose **Preferences**.

Step 3 In the Preferences dialog box under Category, choose **Advanced > Proxies**.

Step 4 On the right side of the Preferences dialog box under Proxies, perform one of the following options:

- Choose **Direct connection to the Internet** to bypass the proxy server.
- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15454 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

NTP-A236 Set Up a Remote Access Connection to the ONS 15454

Purpose	This procedure connects an ONS 15454 using a LAN modem. To complete this procedure: • A modem must be connected to the ONS 15454. • The modem must be provisioned for ONS 15454. To run CTC, the modem must be provisioned for Ethernet access.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Connect the modem to the RJ-45 (LAN) port on the TCC2 card or to the LAN pins on the ONS 15454 backplane.

Step 2 While referring to the modem documentation, complete the following tasks to provision the modem for the ONS 15454:

- For CTC access, set the modem for Ethernet access.
- Assign an IP address to the modem that is on the same subnet as the ONS 15454.
- The IP address the modem assigns to the CTC computer must be on the same subnet as the modem and the ONS 15454.

Note For assistance on provisioning specific modems, contact the Cisco Technical Assistance Center.

Step 3 Continue with the "NTP-A23 Log into the ONS 15454 GUI" procedure on page 3-22.

Stop. You have completed this procedure.

NTP-A23 Log into the ONS 15454 GUI

Purpose	This procedure logs into CTC, the graphical user interface software used to manage the ONS 15454. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-8, or • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-19, or • NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-21
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 If the computer does not have a physical connection to the ONS 15454 or corporate LAN, complete the "DLP-A59 Connect Computer to the ONS 15454" task on page 3-23 or the "NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454" procedure on page 3-19.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24.

Note For information about navigating in CTC, see Appendix A, "CTC Information and Shortcuts."

Step 3 As needed, complete the "DLP-A61 Create Login Node Groups" task on page 3-27. Login node groups allow you to manage nodes that are not connected to the login node via DCC.

Step 4 As needed, complete the "DLP-A62 Add a Node to the Current Session or Login Group" task on page 3-28.

Step 5 As needed, complete the "DLP-A339 Delete a Node from the Current Session or Login Group" task on page 3-29.

Step 6 As needed, complete the "DLP-A431 Change the JRE Version" task on page 3-29.

Step 7 As needed, complete the "DLP-A327 Configure the CTC Alerts Dialog for Automatic Popup" task on page 3-30.

Stop. You have completed this procedure.

DLP-A59 Connect Computer to the ONS 15454

Purpose	This task physically connects a CTC computer to the ONS 15454.
Tools/Equipment	Straight-through (Category 5) LAN cable NIC
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 and one of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-8, or • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-19
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is set up for a local craft connection, connect a straight-through (Category 5) LAN cable from the PC or Solaris workstation NIC to one of the following:

- RJ-45 (LAN) port on the active or standby TCC2 card
- RJ-45 (LAN) port on a hub or switch to which the ONS 15454 is physically connected

Note For instructions on crimping your own straight-through (Category 5) LAN cables, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Note For initial shelf turn up, you should connect your PC directly to the LAN port on the TCC2 card of the ONS 15454.

Step 2 If your computer is set up for a corporate LAN connection, connect a straight-through (Category 5) LAN cable from the PC or Solaris workstation NIC card to a corporate LAN port.

Step 3 Return to your originating procedure (NTP).

DLP-A60 Log into CTC

Purpose	This task logs into CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 One of the following procedures: • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-8, or • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-19, or • NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-21
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For information about CTC views and navigation, see Appendix A, "CTC Information and Shortcuts."

Step 1 From the PC connected to the ONS 15454, start Netscape or Internet Explorer.

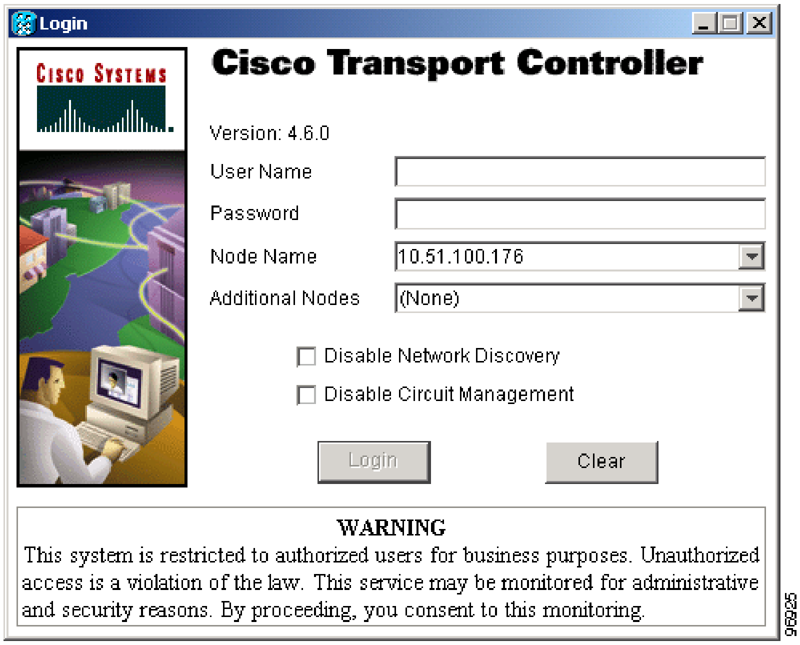
Step 2 In the Netscape or Internet Explorer web address (URL) field, enter the ONS 15454 IP address. For initial setup, this is the default IP address, 192.1.0.2. (This IP address can appear on the LCD. You can suppress the LCD IP address display using CTC. For more information, see the "DLP-A266 Change IP Settings" task on page 12-5.) Press **Enter**.

Note If you are logging into ONS 15454 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE-SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select About CTC from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

If a Java Plug-in Security Warning dialog box appears, complete the "DLP-A418 Install Public-Key Security Certificate" task on page 3-26 to install the public-key security certificate required by Software Release 4.1 and later.

After you complete the security certificate dialog box (or if the certificate is already installed), 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 (Figure 3-1).

Figure 3-1 Logging into CTC



Step 3 In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** and the password **otbu+1**.

> **Note** The CISCO15 user is provided with every ONS 15454. CISCO15 has superuser privileges, so you can create other users. You must create another superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, click the Provisioning > Security tabs after you log in and change the password. To set up ONS 15454 users and assign security, go to the "NTP-A30 Create Users and Assign Security" procedure on page 4-4. Additional information about security is provided in the *Cisco ONS 15454 Reference Manual*.

Step 4 Each time you log into an ONS 15454, you can make selections on the following login options:

- Node Name—Displays the IP address entered in the web browser and a drop-down menu of previously entered ONS 15454 IP addresses. You can select any ONS 15454 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- Additional Nodes—Displays a list of current login node groups. To create a login node group or add additional groups, see the "DLP-A61 Create Login Node Groups" task on page 3-27.

> **Note** The login node group feature supersedes the topology host login feature in found in previous ONS 15454 releases. On upgrade, existing topology host definitions found in by modifying the ctc.ini (Windows) or .ctcrc (UNIX) files are converted to a Topology Host login group.

- Disable Network Discovery—Check this box to view only the ONS 15454 (and login node group members, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.

- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits. This option does not prevent the creation and management of new circuits.

Step 5 Click **Login**.

If the login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15454. If you need to turn up the shelf for the first time, see Chapter 4, "Turn Up Node." If login problems occur, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Return to your originating procedure (NTP).

DLP-A418 Install Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This task is performed during the "DLP-A60 Log into CTC" task on page 3-24. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

Note The Java Plug-in Security Warning dialog box options that appear depend on the JRE version you are using. If you installed JRE 1.4.2, you will see the following options: Yes, No, Always, and More Details. If you are using JRE 1.3.1_02, you will see the following options (noted below in parentheses): Grant This Session, Deny, Grant Always, and View Certificate.

- Yes (Grant This Session)—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454.
- No (Deny)—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15454.
- Always (Grant Always)—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- More Details (View Certificate)—Allows you to view the public-key security certificate.

Step 2 If the Login dialog box appears, continue with Step 3. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file (.java.policy) on your PC. In Software Release 4.0 and earlier, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in Software R4.1 and later, so you can remove it unless you will log into ONS 15454s running software earlier than R4.1. Choose one of the following options:

- Yes—Removes the modified Java policy file from your PC. Choose this option only if you will log into ONS 15454s running Software R4.1 software or later.
- No—Does not remove the modified Java policy file from your PC. Choose this option if you will log into ONS 15454s running Software R4.0 or earlier. If you choose No, this dialog box will appear every time you log into the ONS 15454. If you do not want it to appear, check the **Do not show the message again** check box.

Caution If you delete the Java policy file, you cannot log into nodes running Software R4.0 and earlier. If you delete the file and want to log into an ONS 15454 running an earlier release, insert the software CD for the release into your PC CD-ROM and run the CTC setup wizard to reinstall the Java policy file.

Step 3 Return to your originating procedure (NTP).

DLP-A61 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15454s that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in node view, choose **Preferences**.

Step 2 Click **Login Node Group** and **Create Group**.

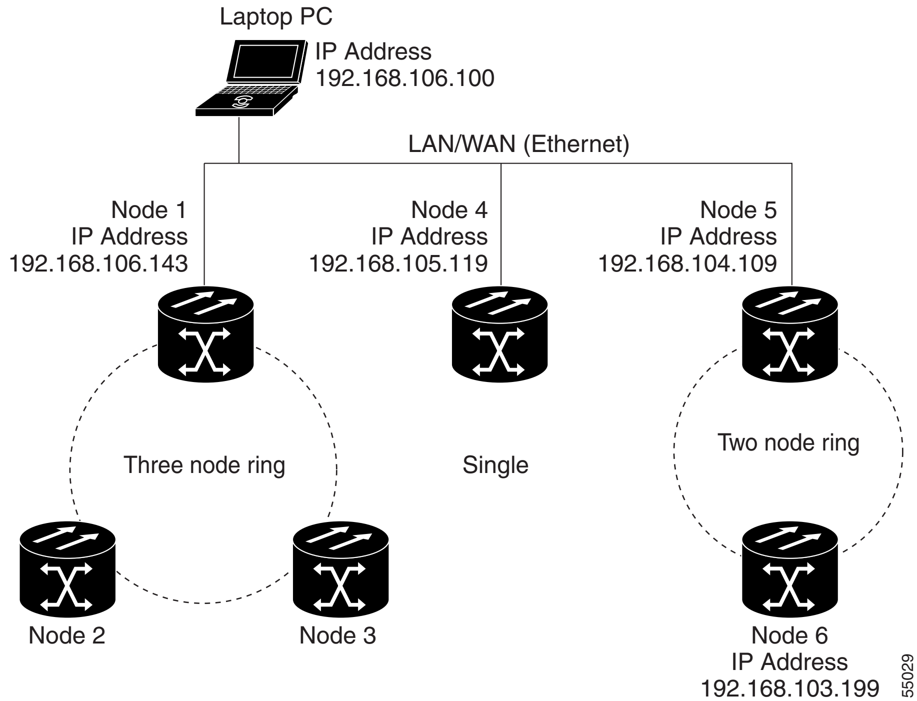
Step 3 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

Step 4 In the Members area, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node that you want to add to the group.

Step 5 Click **OK**.

The next time you log into an ONS 15454, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 3-2, a login node group, “Test Group,” is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose the Test Group group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If Test Group and Disable Network Discovery are both selected, Nodes 1, 4, and 5 appear. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

Figure 3-2 Login Node Group



Step 6 Return to your originating procedure (NTP).

DLP-A62 Add a Node to the Current Session or Login Group

Purpose	This task adds a node to the current CTC session or login node group.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the CTC File menu, click **Add Node**.

Step 2 In the Add Node dialog box, enter the node name (or IP address).

Step 3 If you want to add the node to the current login group, check **Add to current login node group**. Otherwise, leave it unchecked.

Note This check box is active only if you selected a login group when you logged into CTC.

Step 4 Click **OK**.

After a few seconds, the new node appears on the network view map.

Step 5 Return to your originating procedure (NTP).

DLP-A339 Delete a Node from the Current Session or Login Group

Purpose	This task removes a node from the current CTC session or login node group.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the node that you want to delete.

Step 3 From the CTC File menu, click **Delete Selected Node**.

After a few seconds, the node disappears from the network view map.

Step 4 Return to your originating procedure (NTP).

DLP-A431 Change the JRE Version

Purpose	This task changes the JRE version, which is useful if you would like to upgrade to the JRE 1.4.2 version from 1.3.1_02 without using the software or documentation CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.

Step 3 Click the **Browse** button and navigate to the JRE directory on your computer.

Step 4 Choose the JRE version, such as j2re1.4.2_01.

Step 5 Click **OK**.

Step 6 From the File menu, choose **Exit**.

Step 7 In the confirmation dialog box, click **Yes**.

Step 8 Complete the "DLP-A60 Log into CTC" task on page 3-24.

Step 9 Return to your originating procedure (NTP).

DLP-A327 Configure the CTC Alerts Dialog for Automatic Popup

Purpose	This task sets up the CTC Alerts dialog box to open for all alerts, circuit deletion errors only, or never. The CTC Alerts dialog box displays network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the CTC Alerts toolbar icon.

Step 2 In the CTC Alerts dialog box, choose one of the following:

- All alerts—Sets the CTC Alerts dialog box to open automatically for all notifications.
- Error alerts only—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.
- Never—Sets the CTC Alerts dialog box to never open automatically.

Step 3 Click **Close**.

Step 4 Return to your originating procedure (NTP).

CHAPTER 4

Turn Up Node

This chapter explains how to provision a single Cisco ONS 15454 node and turn it up for service, including node name, date and time, timing references, network attributes such as IP address and default router, users and user security, and card protection groups.

If you are provisioning an ONS 15454 for dense wavelength division multiplexing (DWDM) or as a hybrid node (DWDM and TDM), you will not complete some procedures until directed to do so in Chapter 5, “Turn Up a DWDM Node.” These procedures are identified in the procedures list in the following section.

Before You Begin

Complete the procedures applicable to your site plan from the following chapters:

- Chapter 1, “Install the Shelf and Backplane Cable”
- Chapter 2, “Install Cards and Fiber-Optic Cable”
- Chapter 3, “Connect the PC and Log into the GUI”

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A24 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-A30 Create Users and Assign Security, page 4-4—Complete this procedure to create Cisco Transport Controller (CTC) users and assign their security levels.
3. NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-A261 Set Power Monitor Thresholds, page 4-9—Continue with this procedure to set the node battery power thresholds.
5. NTP-A169 Set Up CTC Network Access, page 4-9—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
6. NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-19—Continue with this procedure if the ONS 15454 will be accessed behind firewalls.
7. NTP-A28 Set Up Timing, page 4-22—Continue with this procedure to set up the node’s SONET timing references. If you are turning up a DWDM or hybrid node, do not complete this procedure until directed to do so in Chapter 5, “Turn Up a DWDM Node.”

8. NTP-A170 Create Protection Groups, page 4-26—Complete this procedure, as needed, to set up 1:1, 1:N, 1+1, or Y-cable protection groups for ONS 15454 electrical and optical cards. If you are turning up a DWDM or hybrid node, do not complete this procedure until directed to do so in Chapter 5, "Turn Up a DWDM Node."
9. NTP-A256 Set Up SNMP, page 4-33—Complete this procedure if simple network management protocol (SNMP) will be used for network monitoring.

NTP-A24 Verify Card Installation

Purpose	This procedure verifies that an ONS 15454 node provisioned for SONET is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15454 card installation.
Prerequisite Procedures	Chapter 1, "Install the Shelf and Backplane Cable" Chapter 2, "Install Cards and Fiber-Optic Cable"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that two TCC2 cards are installed in Slots 7 and 11.

Step 2 Verify that the green ACT (active) LED is illuminated on one TCC2 and the amber STBY (standby) LED is illuminated on the second TCC2.

> **Note** If the TCC2 cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A36 Install the TCC2 Cards" task on page 2-7, or refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve installation problems before proceeding to Step 3.

If you are provisioning the ONS 15454 for DWDM, continue with Step 17. Otherwise, continue with the next step.

Step 3 Verify that cross-connect cards (XC, XCVT, or XC10G) are installed in Slots 8 and 10. The cross-connect cards must be the same type.

Step 4 Verify that the green ACT (active) LED is illuminated on one cross-connect card and the amber STBY (standby) LED is illuminated on the second cross-connect card.

> **Note** If the cross-connect cards are not installed, or if their LEDs are not operating as described, do not proceed. Repeat the "DLP-A37 Install the XC, XCVT, or XC10G Cards" task on page 2-9, or refer to the *Cisco ONS 15454 Troubleshooting Manual* to resolve installation problems before proceeding to Step 5.

If you are provisioning the ONS 15454 for DWDM and TDM (hybrid node), continue with Step 17. Otherwise, continue with the next step.

Step 5 If your site plan requires an AIC or AIC-I card, verify that the AIC/AIC-I card is installed in Slot 9 and its ACT (active) LED displays a solid green light.

Step 6 Verify that electrical cards (DS-1, DS-3, EC-1, and DS3XM-6) are installed in Slots 1 to 6 or 12 to 17 as designated by your installation plan.

Step 7 If your site plan requires an Ethernet card, verify that the Ethernet card is installed in the specified slot and its ACT (active) LED displays a solid green light:

- The E100T-12, E100T-12-G, E1000-2, and E1000-2-G cards are installed in Slots 1 to 6 or 12 to 17
- The G1000-4 cards are installed in Slots 1 to 4 or 14 to 17.
- The G1K-4, ML1000-2, and ML100T-12 cards can be installed in Slots 1 to 6 or 12 to 17 if an XC10G cross-connect is installed. However, they must be installed in Slots 5, 6, 12, or 13 if XC or XCVT cards are installed.

Step 8 If Ethernet cards are installed, verify that the correct cross-connect cards are installed in Slots 8 and 10:

- E100T-12-G, E1000-2-G, and G1000-4 cards require XC10G cards.
- G1K-4, ML1000-2, and ML100T-12 cards require XC10G cards if they are installed in Slots 1 to 4 or 14 to 17.

Step 9 If an E1000-2, E1000-2-G, G1000-4, or ML1000-2 Ethernet card is installed, verify that it has a gigabit interface converter (GBIC) or SFP installed. If not, see the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 10 Verify that OC-N cards (OC-3, OC-3-8, OC-12, OC-12-4, OC-48, OC-48 any slot [AS], and OC-192) are installed in the slots designated by your site plan.

- OC-3, OC-12, and OC-48 AS cards can be installed in Slots 1 to 6 or 12 to 17.
- OC-3-8 and OC-12-4 can be installed in Slots 1 to 4 and 14 to 17.
- OC-48 and OC-192 can be installed in Slots 5, 6, 12, or 13.

Step 11 Verify that the correct cross-connect cards are installed in Slots 8 and 10:

- If an OC-192, OC-12-4, or OC-3-8 card is installed, an XC10G card must be installed.
- If an OC-48 AS card is installed in Slots 1 to 4 or 14 to 17, an XC10G card must be installed. If XC or XCVT cards are installed, the OC-48 AS can be installed only in Slots 5, 6, 12, or 13.

Step 12 Verify that all installed OC-N cards display a solid amber STBY LED.

Step 13 If transponder or muxponder cards are installed (TXP_MR_10G, MXP_2.5G_10G, TXP_MR_2.5, or TXPP_MR_2.5G), verify that they are installed in Slots 1 to 6 or 12 to 17 and have GBIC or SFP connectors are installed. If GBICs or SFP connectors are not installed, complete the "DLP-A469 Install GBIC or SFP Connectors" task on page 2-20.

Step 14 If Fibre Channel cards (FC-MR-4) are installed, verify one of the following:

- If XC10G cross-connect cards are installed, the FC-MR-4 is installed in Slots 1 to 6 or 12 to 17 and displays a solid green ACT (Active) LED.
- If XCVT cross-connect cards are installed, the FC-MR-4 is installed in Slots 5 to 6 or 12 to 13 and displays a solid green ACT (Active) LED.

Step 15 Verify that fiber-optic cables (fiber) are installed and connected to the locations indicated in the site plan. If the fiber is not installed, complete the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Step 16 Verify that fiber is routed correctly in the shelf assembly and fiber boots are installed properly. If the fiber is not routed on the shelf assembly, complete the "NTP-A245 Route Fiber-Optic Cables" procedure on page 2-56. If the fiber boots are not installed, complete the "DLP-A45 Install the Fiber Boot" task on page 2-39.

Step 17 Verify that the software release shown on the LCD matches the software release indicated in your site plan. If the release does not match, perform one of the following procedures:

- Perform a software upgrade using a Cisco ONS 15454 software CD. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for instructions.
- Replace the TCC2 cards with cards containing the correct release. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Stop. **You have completed this procedure**.

NTP-A30 Create Users and Assign Security

Purpose	This procedure creates ONS 15454 users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you need to create users. If you are already logged in, continue with Step 2.

Note You must log in as a Superuser to create additional users. The CISCO15 user provided with each ONS 15454 can be used to set up other ONS 15454 users. You can add up to 500 users to one ONS 15454.

Step 2 Complete the "DLP-A74 Create a New User—Single Node" task on page 4-5 or the "DLP-A75 Create a New User—Multiple Nodes" task on page 4-5 as needed.

Note You must add the same user name and password to each node a user will access.

Step 3 If you want to modify the security policy settings, including password aging and idle user timeout policies, complete the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Stop. **You have completed this procedure**.

DLP-A74 Create a New User—Single Node

Purpose	This task creates a new user for one ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 6 to 10 characters.
- Password—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A75 Create a New User—Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15454s.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** > **Users** tabs.

Step 3 In the Users window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must 6 to 10 characters.
- Password—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15454 Reference Manual* for information about the capabilities provided with each level.

Note Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 5 Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5. If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.

Step 8 Return to your originating procedure (NTP).

NTP-A25 Set Up Name, Date, Time, and Contact Information

Purpose	This procedure provisions identification information for the node, including the node name, a contact name and phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 for the node you will turn up. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > General** tabs.

Step 3 Enter the following information in the fields listed:

- Node Name—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric (a-z, A-Z, 0-9) characters.
- Contact—Type the name of the node contact person and the phone number, up to 255 characters (optional).
- Latitude—Enter the node latitude: N (North) or S (South), degrees, and minutes (optional).
- Longitude—Enter the node longitude: E (East) or W (West), degrees, and minutes (optional).

Tip You can also position nodes manually on the network view map. Press Ctrl while you drag and drop the node icon. To create the same network map visible for all ONS 15454 users, complete the "NTP-A172 Create a Logical Network Map" procedure on page 6-52.

CTC uses the latitude and longitude to position ONS 15454 icons on the network view map. To convert a coordinate in degrees to degrees and minutes, multiply the number after the decimal by 60. For example, the latitude 38.250739 converts to 38 degrees, 15 minutes (0.250739 x 60 = 15.0443, rounded to the nearest whole number).

- Description—Type a description of the node. The description can be a maximum of 255 characters.
- Use NTP/SNTP Server—When checked, CTC uses a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node.

  If you do not use an SNTP or NTP server, complete the Date and Time fields. The ONS 15454 will use these fields for alarm dates and times. (CTC displays all alarms in the login node's time zone for cross network consistency.)

  Note Using an NTP or SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

  If you check the Use NTP/SNTP Server check box, type the IP address of one of the following:

  – an NTP/SNTP server connected to the ONS 15454

- Another ONS 15454 with NTP/SNTP enabled that is connected to the ONS 15454

If you check gateway network element (GNE) for the ONS 15454 proxy server (see "DLP-A249 Provision IP Settings" task on page 4-10), external ONS 15454s must reference the gateway ONS 15454 for NTP/SNTP timing. For more information about the ONS 15454 gateway settings, refer to the *Cisco ONS 15454 Reference Manual*.

Caution If you reference another ONS 15454 for the NTP/SNTP server, make sure the second ONS 15454 references an NTP/SNTP server and not the first ONS 15454 (that is, do not create an NTP/SNTP timing loop by having two ONS 15454s reference each other).

- Date—If Use NTP/SNTP Server is not checked, type the current date in the format mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002.
- Time—If Use NTP/SNTP Server is not checked, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15454 uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Click the field and choose a city within your time zone from the drop-down menu. The menu displays the 80 World Time Zones from –11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).
- Use Daylight Savings Time—Check this check box if the time zone that you chose is using Daylight Savings Time.
- Insert AIS-V on STS-1 SD-P—Check this check box if you want AIS-Vs inserted on VT circuits carried by STS-1s when the STS-1 crosses its SD-P BER threshold. On protected circuits, traffic will be switched. If the switch cannot be performed, or if circuits are not protected, traffic will be dropped when the STS-1 SD-P BER threshold is reached.
- SD-P BER—If you selected Insert AIS-V, you can choose the SD-P BER level from the SD-P BER drop-down menu.

Step 4 Click **Apply**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 through 5 to enter the corrections. If the information is correct, continue with the "NTP-A261 Set Power Monitor Thresholds" procedure on page 4-9.

Stop. **You have completed this procedure**.

NTP-A261 Set Power Monitor Thresholds

Purpose	This procedure provisions extreme high, high, extreme low, and low input battery power thresholds within a –48 volts direct current (VDC) environment. When the thresholds are crossed, the TCC2 generates warning alarms in CTC.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 for the node you will set up. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > General > Power Monitor** tabs.

Step 3 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the **ELWBATVGVdc** drop-down menu.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the **LWBATVGVdc** drop-down menu.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the **HIBATVGVdc** drop-down menu.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the **EHIBATVGVdc** drop-down menu.

Step 7 Click **Apply**.

Stop. **You have completed this procedure**.

NTP-A169 Set Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP (Internet Inter-Orb Protocol) listener port, proxy server settings, static routes, Open Shortest Path First (OSPF) protocol, and Routing Information Protocol (RIP).
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A249 Provision IP Settings" task on page 4-10 to provision the ONS 15454 IP address, subnet mask, default router, DHCP server, IIOP listener port, and proxy server settings.

Tip If you cannot log into the node, you can change its IP address, default router, and network mask by using the LCD on the ONS 15454 fan-tray assembly (unless LCD provisioning is suppressed). See the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-13 for instructions. However, you cannot use the LCD to provision any other network settings.

Step 3 If static routes are needed, complete the "DLP-A65 Create a Static Route" task on page 4-15. Refer to the *Cisco ONS 15454 Reference Manual* for further information about static routes.

Step 4 If the ONS 15454 is connected to a LAN or WAN that uses OSPF, complete the "DLP-A250 Set Up or Change Open Shortest Path First Protocol" task on page 4-16.

Step 5 If the ONS 15454 is connected to a LAN or WAN that uses RIP, complete the "DLP-A251 Set Up or Change Routing Information Protocol" task on page 4-18.

Stop. **You have completed this procedure**.

DLP-A249 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, default router, DHCP access, firewall access, and proxy server settings for an ONS 15454 node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution All network changes should be approved by your network (or LAN) administrator.

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the ONS 15454 node.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from being displayed in CTC to users with Provisioner, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)
- LCD IP Display—Choose one of the following:
  - Allow Configuration—Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-13.
  - Display Only—Displays the node IP address on the LCD but does not allow users to change the IP address using the LCD.

- Suppress Display—Suppresses the node IP address display on the LCD.

- Default Router—If the ONS 15454 must communicate with a device on a network that the ONS 15454 is not directly connected to, the ONS 15454 can forward the packets to the default router. Type the IP address of the router in this field.

Note This field is ignored if the node is not connected to a LAN, or if you enable any of the gateway settings to implement the ONS 15454 proxy server feature.

- Forward DHCP Request To—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15454 proxy server features, leave this field blank.

Note If you enable DHCP, computers connected to an ONS 15454 node can obtain temporary IP addresses from an external DHCP server. The ONS 15454 only forwards DHCP requests; it does not act as a DHCP server.

- MAC Address—(*Display only.*) Displays the ONS 15454 IEEE 802 MAC address.
- Net/Subnet Mask Length—Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15454s in the same subnet.
- TCC CORBA (IIOP) Listener Port—Provisions the ONS 15454 IIOP listener port. This listener port enables communication with the ONS 15454 through firewalls. See the "NTP-A27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-19 for more information.
- Gateway Settings—Provides options that enable the ONS 15454 proxy server features. Do not select any of these options until you review the proxy server scenario in the *Cisco ONS 15454 Reference Manual*. In proxy server networks, the ONS 15454 is either an external network element (ENE), gateway network element (GNE), or proxy-only server. Provisioning must be consistent for each NE type.
- Enable proxy server on port—If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454s that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to data communications channel (DCC)-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15454. If Enable proxy server on port is off, the node does not proxy for any CTC clients, although any established proxy connections continue until the CTC client exits. When this box is checked, you can set the node as an ENE or a GNE:
  - External Network Element (ENE)—If selected, the CTC computer is only visible to the ONS 15454 to which the CTC computer is connected. The computer is not visible to other DCC-connected nodes. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
  - Gateway Network Element (GNE)—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.
  - Proxy-only—If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

Both TCC2 cards reboot, one at a time. During this time (approximately 5 minutes), the active and standby TCC2 card LEDs go through the cycle shown in Table 4-1. Eventually, a “Lost node connection, switching to network view” message appears.

Table 4-1 LED Behavior During TCC2 Reboot

Reboot Activity	Active TCC2 LEDs	Standby TCC2 LEDs
Standby TCC2 card updated with new network information. Memory test (1 to 2 minutes). If an AIC or AIC-I card is installed, AIC FAIL and alarm LEDs light up briefly when the AIC is updated. The standby TCC2 becomes the active TCC2.	ACT/STBY: Flashing green.	1. ACT/STBY: Flashing yellow. 2. FAIL LED: Solid red. 3. All LEDs on except ACT/STBY. 4. CRIT turns off. 5. MAJ and MIN turn off. 6. REM, SYNC, and ACO turn off. 7. All LEDs (except A&B PWR) turn off (1 to 2 minutes). 8. ACT/STBY: Solid yellow. 9. Alarm LEDs: Flash once. 10. ACT/STBY: Solid green.
Memory test (1 to 2 minutes). TCC2 updated with new network information. The active TCC2 becomes the standby TCC2.	1. All LEDs: Turn off (1 to 2 minutes). CTC displays “Lost node connection, switching to network view” message. 2. FAIL LED: Solid red. 3. FAIL LED: Flashing red. 4. All LEDs on except ACT/STBY. 5. CRIT turns off. 6. MAJ and MIN turn off. 7. REM, SYNC, and ACO turn off; all LEDs are off. 8. ACT/STBY: Solid yellow. 9. ACT/STBY: Flashing yellow. 10. ACT/STBY: Solid yellow.	ACT/STBY: Solid green.

Step 5 Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.

Step 6 Double-click the node icon when it becomes green.

Step 7 Return to your originating procedure (NTP).

DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the ONS 15454 IP address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	Optional
Onsite/Remote	Onsite
Security Level	None

Note You cannot perform this task if the LCD IP Display on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See "DLP-A249 Provision IP Settings" task on page 4-10 to view or change the LCD IP Display field.

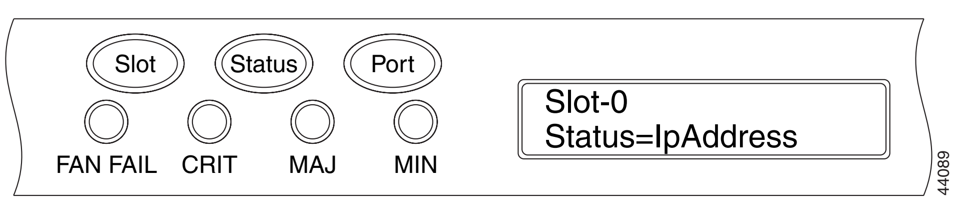
Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until Node appears on the LCD.

Step 2 Repeatedly press the **Port** button until the following displays:

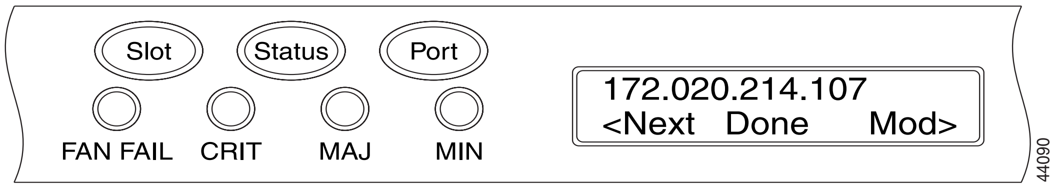
- To change the node IP address, Status=IpAddress (Figure 4-1)
- To change the node network mask, Status=Net Mask
- To change the default router IP address, Status=Default Rtr

Figure 4-1 Selecting the IP Address Option



Step 3 Press the **Status** button to display the node IP address (Figure 4-2), the node subnet mask length, or the default router IP address.

Figure 4-2 Changing the IP Address



Step 4 Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

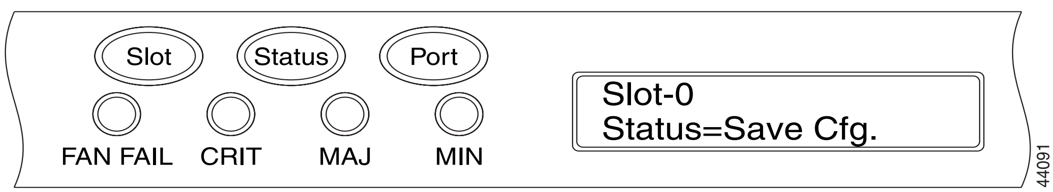
Tip The Slot, Status, and Port button positions correspond to the command position on the LCD. For example, in Figure 4-2, you press the Slot button to invoke the Next command and the Port button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address or subnet mask to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the Node menu.

Step 7 Repeatedly press the **Port** button until the Save Configuration option appears (Figure 4-3).

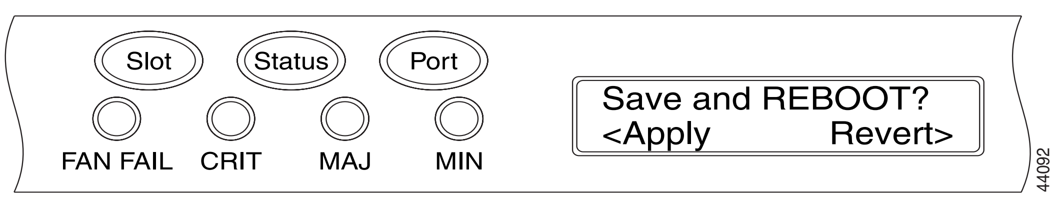
Figure 4-3 Selecting the Save Configuration Option



Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears (Figure 4-4).

Figure 4-4 Saving and Rebooting the TCC2



Step 9 Press the **Slot** button to apply the new IP address configuration or press **Port** to cancel the configuration.

Saving the new configuration causes the TCC2 cards to reboot. During the reboot, a "Saving Changes - TCC Reset" message displays on the LCD. The LCD returns to the normal alternating display after the TCC2 reboot is complete (see Table 4-1 on page 4-12 for reboot behavior).

Note The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

Step 10 Return to your originating procedure (NTP).

DLP-A65 Create a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required if either of the following conditions are is true: • CTC computers on one subnet need to connect to ONS 15454s that are connected by a router to ONS 15454s residing on another subnet. OSPF is not enabled and the External Network Element gateway setting is not checked. • You need to enable multiple CTC sessions among ONS 15454s residing on the same subnet and the External Network Element gateway setting is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab. Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15454 and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note Static route networking examples are provided in the IP networking section of the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A250 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the Open Shortest Path First (OSPF) routing protocol on the ONS 15454. Perform this task if you want to include the ONS 15454 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15454 is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 On the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15454s as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 10. The metric changes to 100 if you check the OSPF Active on LAN check box in Step 3.
- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

Step 3 In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables the ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454s that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15454 is connected. (This number is different from the DCC/GCC OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

   - Type—Choose **Simple Password**.
   - Enter Authentication Key—Enter the password.
   - Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Provision the OSPF priority and interval settings.

The OSPF priority and interval defaults are ones most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the ONS 15454 is connected.

- Router Priority—Selects the designated router for a subnet.
- Hello Interval (sec)—Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Indicates the service speed. One second is the default.
- Retransmit Interval (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Sets a cost for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Step 6 Under OSPF Area Range Table, create an area range table if one is needed:

Note Area range tables consolidate the information that is outside an OSPF area border. One ONS 15454 in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:
   - Range Address—Enter the area IP address for the ONS 15454s that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
   - Range Area ID—Enter the OSPF area ID for the ONS 15454s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
   - Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
   - Advertise—Check if you want to advertise the OSPF range table.

c. Click **OK**.

Step 7 All OSPF areas must be connected to Area 0. If the ONS 15454 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

a. Under OSPF Virtual Link Table, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields. OSPF settings must match OSPF settings for the ONS 15454 OSPF area:
   - Neighbor—The router ID of the Area 0 router.
   - Transit Delay (sec)—The service speed. One second is the default.
   - Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
   - Auth Type—If the router where the ONS 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
   - Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
   - Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 8 After entering ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the TCC2 cards reset, one at a time. The reset takes approximately 10 to 15 minutes. Table 4-1 on page 4-12 shows the LED behavior during the TCC2 reset.

Step 9 Return to your originating procedure (NTP).

DLP-A251 Set Up or Change Routing Information Protocol

Purpose	This task enables Routing Information Protocol (RIP) on the ONS 15454. Perform this task if you want to include the ONS 15454 in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 You need to create a static route to the router adjacent to the ONS 15454 for the ONS 15454 to communicate its routing information to non-DCC-connected nodes.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the drop-down menu, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the ONS 15454 is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a. Click the **No Authentication** button.

b. In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password,
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15454 is a gateway NE with multiple external ONS 15454 NEs attached with IP addresses in different subnets.

a. In the RIP Address Summary area, click **Create**.

b. In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.

- Mask Length—Enter the subnet mask length using the up and down arrows.
- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c. Click **OK.**

Step 7 Return to your originating procedure (NTP).

NTP-A27 Set Up the ONS 15454 for Firewall Access

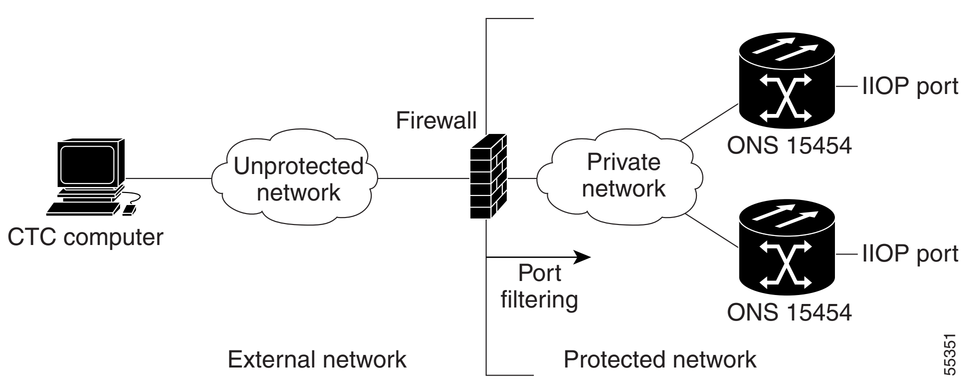
Purpose	This procedure provisions ONS 15454s and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node that is behind the firewall. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A67 Provision the IIOP Listener Port on the ONS 15454" task on page 4-20.

Figure 4-5 shows ONS 15454s in a protected network and the CTC computer in an external network. For the computer to access the ONS 15454s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15454.

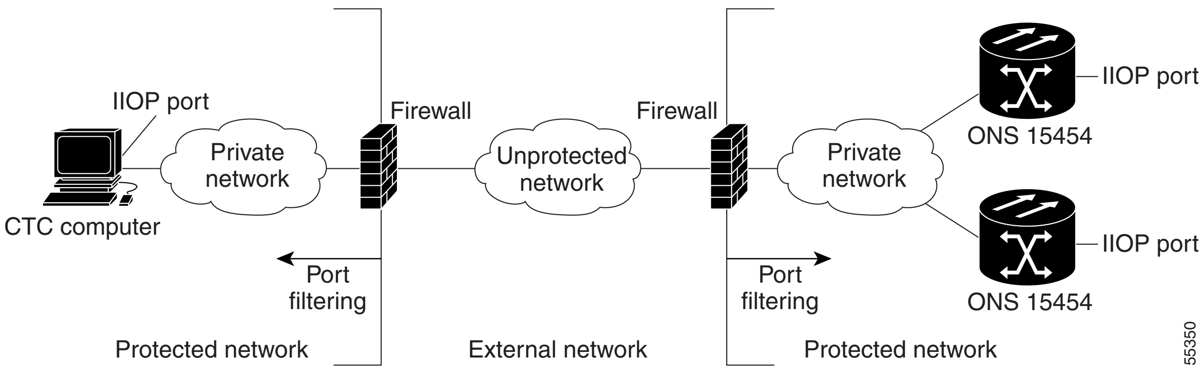
Figure 4-5 Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-A68 Provision the IIOP Listener Port on the CTC Computer" task on page 4-22.

Figure 4-6 shows a CTC computer and ONS 15454 behind firewalls. For the computer to access the ONS 15454, you must provision the IIOP port on the CTC computer and on the ONS 15454.

Figure 4-6 CTC Computer and ONS 15454s Residing Behind Firewalls



Stop. You have completed this procedure.

DLP-A67 Provision the IIOP Listener Port on the ONS 15454

Purpose	This task sets the IIOP listener port on the ONS 15454, which enables you to access ONS 15454s that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable Proxy Server on port 1080 check box is checked, CTC will use port 1080 and ignore the configured IIOP port setting. If Enable Proxy Server is subsequently unchecked, the configured IIOP listener port will be used.

Step 1 In node view, click the **Provisioning** > **Network** > **General** tabs.

Step 2 In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - TCC Fixed—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Uses Port 683, the CORBA default port number.
- Other Constant—If Port 683 is not used, type the IIOP port specified by your firewall administrator. The port cannot use any of the ports shown in Table 4-2.

Table 4-2 Ports Used by the TCC2 Cards

Port	Function
0	Reserved
21	FTP control
23	Telnet
80	HTTP
111	rpc (not used; but port is in use)
513	rlogin (not used; but port is in use)
=<1023	Default CTC listener ports
1080	Proxy server
2001-2017	I/O card telnet
2018	DCC processor on active TCC2
2361	TL1
3082	TL1
3083	TL1
5001	Bidirectional line switched ring (BLSR) server port
5002	BLSR client port
7200, 7209, 7210	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC2 boot port
9999	Flash manager
57790	Default TCC2 listener port

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

Both ONS 15454 TCC2s reboot, one at a time. The reboot takes approximately 15 minutes. See Table 4-1 on page 4-12.

Step 5 Return to your originating procedure (NTP).

DLP-A68 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required only if the computer running CTC resides behind a firewall.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Firewall** tab.

Step 3 In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - Variable—Use to connect to ONS 15454s from within a firewall or if no firewall is used (default).
- Standard Constant—Use Port 683, the CORBA default port number.
- Other Constant—If Port 683 is not used, enter the IIOP port defined by your administrator.

Step 4 Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 In the Preferences dialog box, click **OK**.

Step 7 To access the ONS 15454 using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit from the File menu.**)

Step 8 Return to your originating procedure (NTP).

NTP-A28 Set Up Timing

Purpose	This procedure provisions the ONS 15454 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the ONS 15454 is a DWDM or hybrid (TDM and DWDM) node, do not complete this procedure if you are provisioning the node for line timing with an OSCM or OSC-CSM card as a timing reference. The OSCM and OSC-CSM are not available for selection on the Timing subtab until you complete the "NTP-A268 Install the DWDM or Hybrid Node Cards" procedure on page 5-3. If the DWDM or hybrid node timing is external, that is, timing is derived from a BITS source wired to the backplane, you can complete this procedure now.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will set up timing. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A69 Set Up External or Line Timing" task on page 4-23 if an external building integrated timing supply (BITS) source is available. This is the common SONET timing setup procedure.

Step 3 If you cannot complete Step 2 (an external BITS source is not available), complete the "DLP-A70 Set Up Internal Timing" task on page 4-25. This task can only provide Stratum 3 timing.

> **Note** For information about SONET timing, refer to the *Cisco ONS 15454 Reference Manual* or to Telcordia GR-253-CORE.

Stop. **You have completed this procedure**.

DLP-A69 Set Up External or Line Timing

Purpose	This task defines the SONET timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing area, complete the following information:

- Timing Mode—Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card (non-DWDM nodes) or OSC card (DWDM nodes) that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references.

  > **Note** Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- SSM Message Set—Choose a synchronization status messaging (SSM) message set. All ONS 15454s can translate Generation 2 message sets, so choose Generation 2 if the ONS 15454 is connected to other ONS 15454s. Choose Generation 1 only when the ONS 15454 is connected to equipment that does not support Generation 2. If a node that has its SSM Message Set set to Generation 1 receives a Generation 2 message, it maps the message down to the next available Generation 1 message. The transit node clock (TNC) and ST3E (Stratum 3E) will become an ST3 (Stratum 3).

- Quality of RES—If your timing source supports the reserved S1 byte, set the timing quality here. (Most timing sources do not use RES.) Qualities are displayed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. Refer to the *Cisco ONS 15454 Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Revertive Time—If Revertive is checked, choose the amount of time the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

Step 3 In the BITS Facilities area, complete the following information:

> **Note** The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service) depending whether one or both BITS input pin pairs on the backplane are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).
- BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.

Step 4 If the BITS In State for BITS-1 and BITS-2 is set to OOS, continue with Step 5. If the BITS In State is set to IS for either BITS-1 or BITS-2, complete the following information:

- Coding—Set to the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- Framing—Set to the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).
- Sync Messaging—Check to enable SSM. SSM is not available if Framing is set to SF (D4).
- AIS Threshold—If SSM is disabled or SF (D4) is used, set the quality level where a node sends an alarm indication signal (AIS) from the BITS-1 Out and BITS-2 Out backplane pins. An AIS is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—If you are timing an external device connected to the BITS Out pins, set the distance between the device and the ONS 15454. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft. Line build out (LBO) relates to the BITS cable length.

Step 5 In the Reference Lists area, complete the following information:

> **Note** Reference Lists defines up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

Note If a 1+1 node will use line timing, make a working OC-N card the Ref-X timing source. The system will automatically choose the corresponding protect OC-N card as the Ref-X protect timing source. This will be visible in the Maintenance > Timing tab.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. Reference 3 is the Stratum 3 clock provided on the TCC2 card. The options displayed depend on the Timing Mode setting.
  - If the Timing Mode is set to External, your options are BITS-1, BITS-2, and Internal Clock.
  - If the Timing Mode is set to Line, your options are the node's working OC-N cards (non-DWDM nodes) or OSC cards (DWDM nodes) and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
  - If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk cards as timing references.
- BITS-1 Out/BITS-2 Out—Sets the timing references for equipment wired to the BITS Out backplane pins. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to external, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 6 Click **Apply**.

Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

Step 7 Return to your originating procedure (NTP).

DLP-A70 Set Up Internal Timing

Purpose	This task sets up internal timing (Stratum 3) for an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed (use only if a BITS source is not available)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing area, enter the following:

- Timing Mode—Set to External.
- SSM Message Set—Set to Generation 1.
- Quality of RES—Does not apply to internal timing.
- Revertive—Does not apply to internal timing.
- Revertive Time—Does not apply to internal timing.

Step 3 In the BITS Facilities area, change BITS In State and BITS Out State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.

Step 4 In the Reference Lists area, enter the following information:

- NE Reference
  - Ref 1—Set to Internal Clock.
  - Ref 2—Set to Internal Clock.
  - Ref 3—Set to Internal Clock.
- BITS-1 Out/BITS-2 Out—Set to None.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

NTP-A170 Create Protection Groups

Purpose	This procedure creates ONS 15454 card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 Complete one or more of the following tasks depending on the protection groups you want to create:

- DLP-A71 Create a 1:1 Protection Group, page 4-28
- DLP-A72 Create a 1:N Protection Group, page 4-29
- DLP-A73 Create a 1+1 Protection Group, page 4-30
- DLP-A252 Create a Y-Cable Protection Group, page 4-32

Table 4-3 describes the protection types available on the ONS 15454.

Table 4-3 Protection Types

Type	Cards	Description and Installation Requirements
1:1	DS1-14 DS3-12 DS3-12E EC1-12 DS3XM-6	Pairs one working card with one protect card. The protect card should be installed in an odd-numbered slot and the working card in an even-numbered slot next to the protect slot towards the TCC2, for example: protect in Slot 1, working in Slot 2; protect in Slot 3, working in Slot 4; protect in Slot 15, working in Slot 14. 1:1 protection can be revertive or nonrevertive. For more information, refer to the "Card Protection" chapter in the *ONS 15454 Reference Manual*.
1:N	DS1N-14 DS3N-12 DS3N-12E	Assigns one protect card for several working cards. The maximum is 1:5. Protect cards (DS1N-14, DS3N-12, DS3N-12E) must be installed in Slots 3 or 15 and the cards they protect must be on the same side of the shelf. Protect cards must match the cards they protect. For example, a DS1N-14 can only protect DS1-14 or DS1N-14 cards. If a failure clears, traffic reverts to the working card after the reversion time has elapsed. For more information, refer to the "Card Protection" chapter in the *ONS 15454 Reference Manual*.
1+1	Any OC-N	Pairs a working OC-N card/port with a protect OC-N card/port. For multiport OC-N cards, the protect port must match the working port on the working card. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. The ports on multiport cards must be either working or protect. You cannot mix working and protect ports on the same card. Cards do not need to be in adjoining slots. 1+1 protection can be revertive or nonrevertive, bidirectional or unidirectional.
Y Cable	MXP_2.5_10G TXP_MR_10G TXP_MR_2.5G	Pairs a working transponder or muxponder card/port with a protect transponder or muxponder card/port. The protect port must be on a different card than the working port and it must be the same card type as the working port. The working and protect port numbers must be the same, that is, Port 1 can only protect Port 1, Port 2 can only protect Port 2, etc.
Splitter	TXPP_MR_2.5G	Splitter protection is automatically provided with the TXPP_MR_2.5G card.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15454. Unprotected is the default protection type.

Stop. You have completed this procedure.

DLP-A71 Create a 1:1 Protection Group

Purpose	This task creates a 1:1 electrical card protection group.
Tools/Equipment	Redundant DS-1, DS-3, EC-1, or DS3XM-6 cards should be installed in the shelf, or the ONS 15454 slots must be provisioned for two of these cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards required for 1:1 protection are installed according to requirements specified in Table 4-3.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

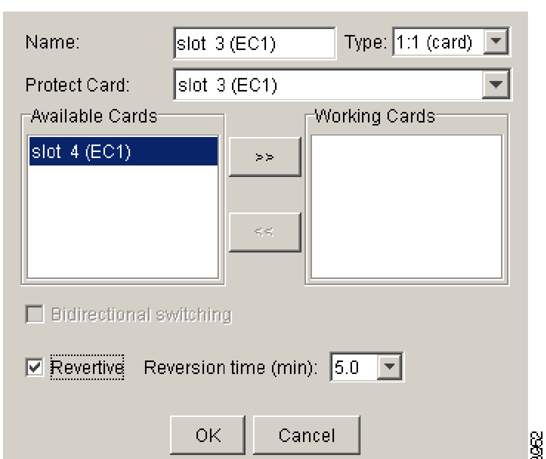
Step 3 Click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:1** from the drop-down menu.
- Protect Card—Choose the protect card from the drop-down menu. The menu displays cards available for 1:1 protection. If no cards are available, no cards appear in the list.

After you choose the protect card, the card available for protection appear in the Available Cards list, as shown in Figure 4-7. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-7 Creating a 1:1 Protection Group



Step 5 From the Available Cards list, choose the card that will be protected by the card selected in the Protect Card drop-down menu. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:1 protection.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, choose the reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A72 Create a 1:N Protection Group

Purpose	This task creates a DS-1 or DS-3 1:N protection group.
Tools/Equipment	DS1N-14, DS3N-12, or DS3N-12E (protect cards) in Slot 3 or Slot 15; DS1-14, DS3-12, or DS3-12E (working cards) installed on either side of a corresponding protect card.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to the 1:N requirements specified in Table 4-3 on page 4-27.

Step 2 Click the **Provisioning** > **Protection** tabs.

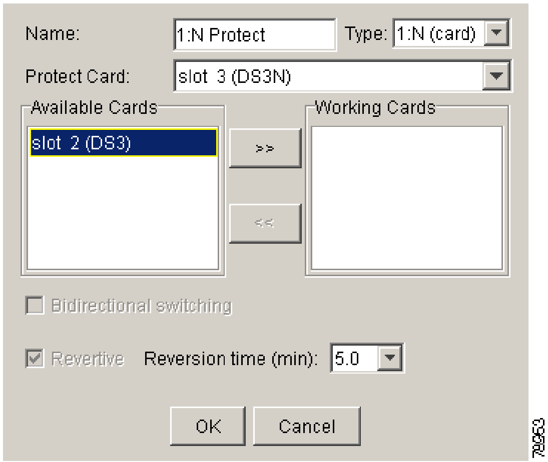
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (“) characters.
- Type—Choose **1:N** from the drop-down menu.
- Protect Card—Choose the protect card from the drop-down menu. The menu displays DS1N-14, DS3N-12, or DS3N-12E cards installed in Slots 3 or 15. If these cards are not installed, no cards appear in the drop-down menu.

After you choose the protect card, a list of cards available for protection appear in the Available Cards list, as shown in Figure 4-8. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-8 Creating a 1:N Protection Group



Step 5 From the Available Cards list, choose the cards that will be protected by the card selected in the Protect Card drop-down menu. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Not available for 1:N protection.
- Revertive—Always enabled for 1:N protection groups.
- Reversion time—Click **Reversion time** and select a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A73 Create a 1+1 Protection Group

Purpose	This task creates a 1+1 protection group for any OC-N card/port (OC-3, OC-3-8, OC-12, OC-12-4, OC-48, OC-48 AS, and OC-192).
Tools/Equipment	Installed OC-N cards or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to 1+1 requirements specified in Table 4-3 on page 4-27.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

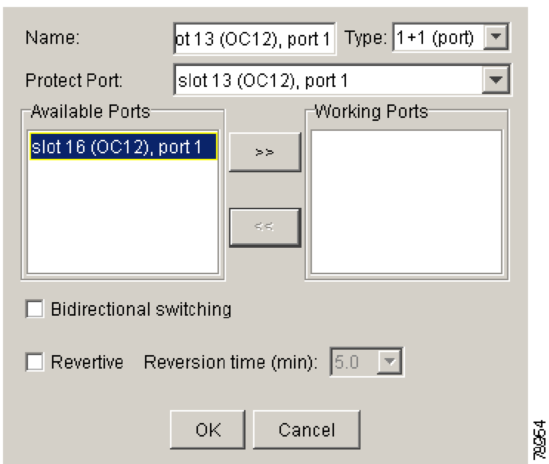
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
- Type—Choose **1+1** from the drop-down menu.
- Protect Port—Choose the protect port from the drop-down menu. The menu displays the available OC-N ports, as shown in Figure 4-9. If OC-N cards are not installed, no ports appear in the drop-down menu.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in Figure 4-9. If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the "DLP-A330 Preprovision a Slot" task on page 5-5.

Figure 4-9 Creating a 1+1 Protection Group



Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Check this check box if you want both Tx and Rx signals to switch to the protect port when a failure occurs to one signal. Leave unchecked if you want only the failed signal to switch to the protect port.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-A252 Create a Y-Cable Protection Group

Purpose	This task creates a Y-cable protection group between the client ports of two transponder (TXP_MR_10G or TXP_MR_2.5G) or two muxponder (MXP_2.5G_10G) cards.
Tools/Equipment	Installed transponder or muxponder cards or preprovisioned slots.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Loss of Pointer Path (LOP-P) alarms can occur on a split signal if the ports are not in a Y-cable protection group.

Step 1 Verify that the transponder or muxponder cards are installed according to the Y-cable requirements specified in Table 4-3 on page 4-27.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

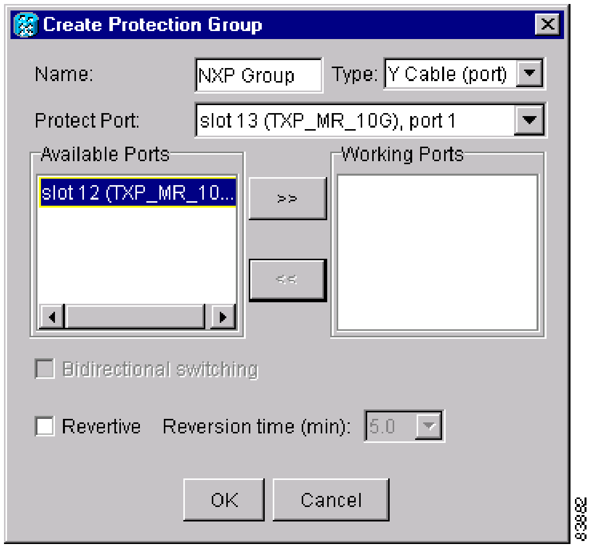
Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question mark (?), backslash (\), or double quote (“) characters.
- Type—Choose **Y Cable** from the drop-down menu.
- Protect Port—Choose the protect port from the drop-down menu. The menu displays the available transponder or muxponder ports, as shown in Figure 4-9. If transponder or muxponder cards are not installed, no ports appear in the drop-down menu.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in Figure 4-10. If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “DLP-A330 Preprovision a Slot” task on page 5-5.

Figure 4-10 Creating a Y-Cable Protection Group



Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in Protect Ports. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Revertive—Check this check box if you want traffic to revert to the working port after failure conditions remain corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, select a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

NTP-A256 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required if SNMP is used at your installation.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning** > **SNMP** tabs.

Step 3 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.

Step 4 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box located on the SNMP tab.

Step 5 Click **Apply**.

Step 6 After clicking either one or both option check boxes, click **Create** in the Trap Destinations area.

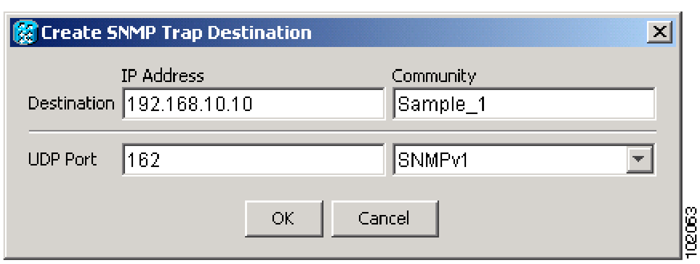
Step 7 If you are only allowing SNMP sets, complete the following in the Create SNMP Trap Destination dialog box (Figure 4-11):

- Destination IP Address—Type the IP address of your network management system. If the node you are logged into is an ENE, set the destination address to the GNE.
- Community—Type the SNMP community name. For a description of SNMP community names, refer to the SNMP information in the *Cisco ONS 15454 Reference Manual*.

  Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system (NMS).

- UDP Port—The default User Datagram Protocol (UDP) port for SNMP is 162. If the node is an ENE in a proxy server network, the UDP port must be set to the GNE's SNMP relay port, which is 391 for SNMPv1.
- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

Figure 4-11 Creating an SNMP Trap Without Proxy



Step 8 Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.

Step 9 Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.

Step 10 If you are enabling SNMP proxy, the dialog box contains additional fields that allow you to set three relays addresses for sending SNMP trap error counts back to NE. To complete these relay IP address fields:

a. Click the first trap destination IP address. The address and its community name appear in the Destination fields.

b. Enter up to three SNMP Proxy relay addresses and community names in the fields for Relay A, Relay B, and Relay C.

Note The community names specified for each relay node must match one of the provisioned SNMP community names in the NE.

Note The SNMP proxy directs SNMP traps from this node through IpA to IpB to IpC to the trap destination. Ensure that you enter the IP addresses in the correct order so that this sequence runs correctly.

Step 11 Click **OK**.

Stop. **You have completed this procedure**.

CHAPTER 5

Turn Up a DWDM Node

This chapter explains how to provision a single Cisco ONS 15454 dense wavelength division multiplexing (DWDM) or a single hybrid (TDM and DWDM) node and turn it up for service, including node name, date and time, timing references, network attributes such as IP address and default router, users and user security, card installation, and DWDM connections.

Note Procedures in this chapter require Cisco MetroPlanner, a DWDM planning tool provided to you by your Cisco account representative. You enter your DWDN network topology and traffic requirements into MetroPlanner. MetroPlanner prepares a shelf plan for each network node and calculates the power and attenuation levels for the DWDM cards installed in the node. For information about Cisco MetroPlanner, contact your Cisco account representative.

Before You Begin

Complete the procedures and tasks listed in Table 5-1 for the node type you are provisioning (DWDM or hybrid) before starting procedures in this chapter:

Table 5-1 DWDM and Hybrid Node Installation Road Map

Chapter	DWDM Node	Hybrid (TDM and DWDM) Node
Chapter 1, "Install the Shelf and Backplane Cable"	All procedures and tasks	All procedures and tasks
Chapter 2, "Install Cards and Fiber-Optic Cable"	DLP-A36 Install the TCC2 Cards, page 2-7	1. DLP-A36 Install the TCC2 Cards, page 2-7 2. DLP-A37 Install the XC, XCVT, or XC10G Cards, page 2-9

Table 5-1 DWDM and Hybrid Node Installation Road Map (continued)

Chapter	DWDM Node	Hybrid (TDM and DWDM) Node
Chapter 3, "Connect the PC and Log into the GUI"	All procedures and tasks	All procedures and tasks
Chapter 4, "Turn Up Node"	1. *NTP-A24 Verify Card Installation, page 4-2* 2. *NTP-A30 Create Users and Assign Security, page 4-4* 3. NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7 4. NTP-A169 Set Up CTC Network Access, page 4-9 5. NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-19 6. NTP-A28 Set Up Timing, page 4-22[1] 7. *NTP-A256 Set Up SNMP, page 4-33*	1. *NTP-A24 Verify Card Installation, page 4-2* 2. *NTP-A30 Create Users and Assign Security, page 4-4* 3. NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7 4. NTP-A169 Set Up CTC Network Access, page 4-9 5. NTP-A27 Set Up the ONS 15454 for Firewall Access, page 4-19 6. NTP-A28 Set Up Timing, page 4-22[1] 7. *NTP-A256 Set Up SNMP, page 4-33*

1. External timing only; line timing with an OSCM or OSC-CSM timing reference is performed in this chapter.

This section lists the procedures (NTPs) that you need to complete to turn up a DWDM node. Turn to a procedure for applicable tasks (DLPs).

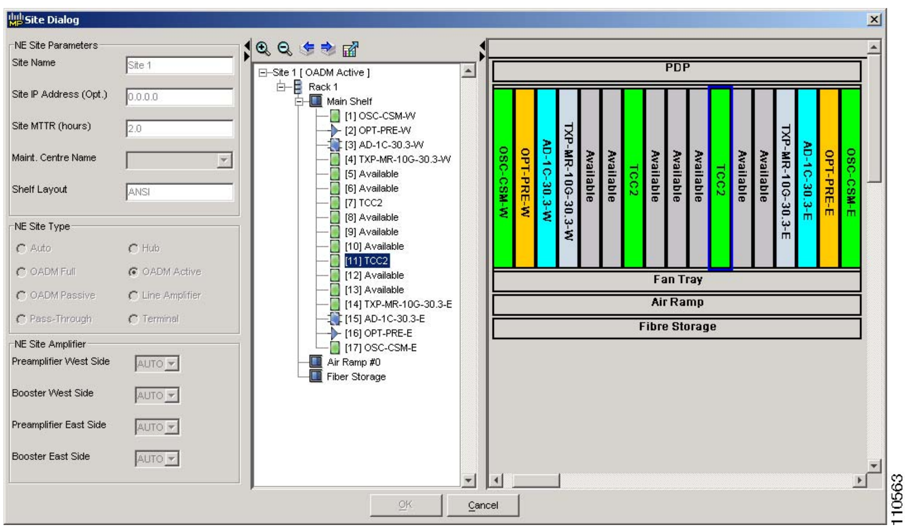
1. NTP-A268 Install the DWDM or Hybrid Node Cards, page 5-3—Complete this procedure first.
2. NTP-A269 Provision the DWDM Connections, page 5-5—Complete this procedure next.
3. NTP-A270 Run Automatic Node Setup, page 5-9—Complete this procedure next.
4. NTP-A271 Verify OSCM and OSC-CSM Transmit Power, page 5-12—Complete this procedure next.
5. NTP-A273 Terminal and Hub Node Acceptance Test, page 5-13—Complete this procedure to test terminal and hub nodes.
6. NTP-A272 View DWDM Node Parameters, page 5-15—Complete this procedure, as needed, to view or modify DWDM parameters.

NTP-A268 Install the DWDM or Hybrid Node Cards

Purpose	This procedure installs cards in DWDM or hybrid (DWDM and TDM) nodes.
Tools/Equipment	None
Prerequisite Procedures	A DWDM network plan calculated by Cisco MetroPlanner. MetroPlanner is a planning tool available from your Cisco account representative that calculates the DWDM card locations based on your network topology and traffic requirements.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In MetroPlanner, display the NE Site Dialog for the node you are provisioning (Figure 5-1).

Figure 5-1 MetroPlanner NE Site Dialog



Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the DWDM node you want to provision.

Step 3 Complete the "DLP-A330 Preprovision a Slot" task on page 5-5 for each DWDM card based on the NE site parameters provided by MetroPlanner.

Step 4 If your site plan requires AIC, AIC-I, transponder (TXP) or muxponder (MXP) cards, complete the following procedures and tasks. If not, continue with Step 5.

- To install AIC or AIC-I cards, complete the "DLP-A38 Install the Alarm Interface Controller or Alarm Interface Controller–International Card" task on page 2-11.
- To install TXP and MXP cards, complete the "NTP-A249 Install the Transponder and Muxponder Cards" procedure on page 2-14.

Note The MetroPlanner NE site plan does not show AIC and AIC-I card locations.

Step 5 Install the DWDM cards in their preprovisioned slots. See the "NTP-A242 Install the DWDM Cards" procedure on page 2-25.

Step 6 If OPT-PRE (amplifier) cards are installed, perform one of the following:

- If dispersion compensating cards (DCUs) are required, install the DCUs in the DCU shelf assembly according to the NE site plan provided by MetroPlanner. See the "NTP-A243 Install the DWDM Dispersion Compensating Cards" procedure on page 2-28.
- If DCUs are not required, connect the two OPT-PRE DC ports with the attenuated patch cord shipped with the OPT-PRE card.

Note If the DCU chassis is not installed, complete the "DLP-A412 Install the DCU Shelf Assembly" task on page 1-65.

Step 7 If transponder or muxponder cards are installed and your site plan requires Y cable protection, complete the "DLP-A252 Create a Y-Cable Protection Group" task on page 4-32. If not, continue with Step 9.

Step 8 (hybrid nodes only) Install the OC-N and DS-N cards using the following procedures:

- NTP-A16 Install the OC-N Cards, page 2-12
- NTP-A17 Install the Electrical Cards, page 2-16

Step 9 (hybrid nodes only) If OC-N or electrical cards are installed and your site plan requires card protection, complete one or more of the following tasks. If not, continue with Step 10.

- DLP-A71 Create a 1:1 Protection Group, page 4-28 for 1:1 electrical card protection.
- DLP-A72 Create a 1:N Protection Group, page 4-29 for 1:N electrical card protection.
- DLP-A73 Create a 1+1 Protection Group, page 4-30 for 1+1 OC-N card protection.

Step 10 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Stop. **You have completed this procedure**.

DLP-A330 Preprovision a Slot

Purpose	This task preprovisions a card slot in CTC before you physically install the card in the ONS 15454. You can use this task for TDM, DWDM, and hybrid nodes.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, right-click the empty slot where you will later install a card.

Step 2 From the Add Card popup menu, choose the card type that will be installed. Only cards that can be installed in the slot appear in the Add Card popup menu.

Note When you preprovision a slot, the card appears purple in the CTC shelf graphic, rather than white when a card is installed in the slot. NP (not present) on the card graphic indicates that the card is not physically installed.

Step 3 Return to your originating procedure (NTP).

NTP-A269 Provision the DWDM Connections

Purpose	This procedure provisions an ONS 15454 connections for ONS 15454s provisioned for DWDM or DWDM and TDM (hybrid).
Tools/Equipment	None
Prerequisite Procedures	A DWDM network plan calculated by Cisco MetroPlanner.
	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 3 Complete the "DLP-A389 Connect the Internal DWDM Cables" task on page 5-6.

Step 4 Complete the "DLP-A396 Calculate DWDM Connections" task on page 5-8.

Stop. You have completed this procedure.

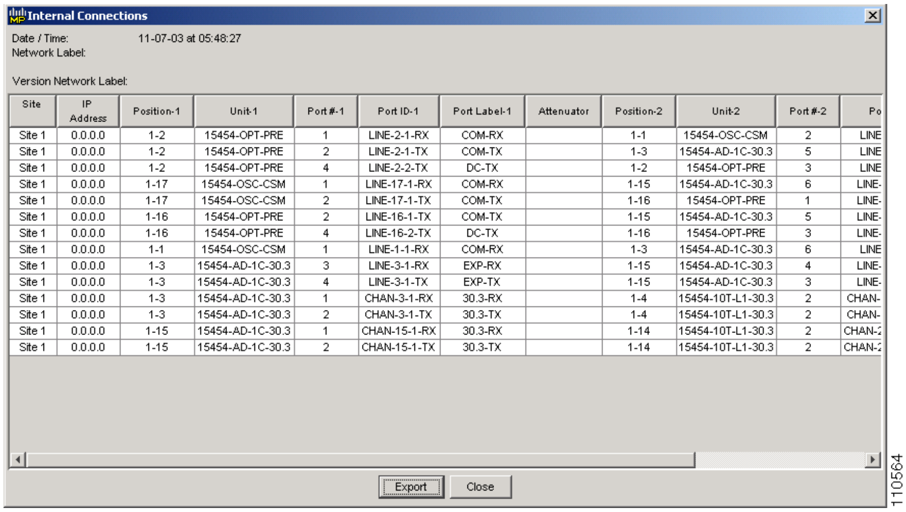
DLP-A389 Connect the Internal DWDM Cables

Purpose	This task connects the internal ONS 15454 cables for ONS 15454s provisioned for DWDM or DWDM and TDM (hybrid).
Tools/Equipment	None
Prerequisite Procedures	A DWDM network plan calculated by Cisco MetroPlanner.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In MetroPlanner, display the Internal Connections table for the node you are provisioning (Figure 5-2 on page 5-7). The internal connections table shows the following information:

- Site 1—The DWDM network site number for the node where you are provisioning the internal connections.
- IP Address—The node IP address.
- Position-1—The first (west) position site and slot. For example, "1-2" indicates site 1, slot 2.
- Unit-1—The ONS 15454 DWDM card (unit) that is installed in the first position slot.
- Port #1—The card port number used for the first Position-1 connection.
- Port ID-1—The port ID used for the Position-1 connection.
- Port Label-1—The port label for the Position-1 connection.
- Attenuator—Indicates whether attenuation is required.
- Position-2—The second (east) position site and slot. For example, "1-1" indicates site 1, slot 1.
- Unit-2—The ONS 15454 DWDM card (unit) that is installed in the Position-2 slot.
- Port #2—The card port number used for the Position-2 connection.
- Port ID-1—The port ID used for the Position-2 connection.
- Port Label-1—The port label for the Position-2 connection.
- Manually Set—Indicates whether you must create the connection manually.

Figure 5-2 MetroPlanner Internal Connections Table



Site	IP Address	Position-1	Unit-1	Port #-1	Port ID-1	Port Label-1	Attenuator	Position-2	Unit-2	Port #-2	Po
Site 1	0.0.0.0	1-2	15454-OPT-PRE	1	LINE-2-1-RX	COM-RX		1-1	15454-OSC-CSM	2	LINE
Site 1	0.0.0.0	1-2	15454-OPT-PRE	2	LINE-2-1-TX	COM-TX		1-3	15454-AD-1C-30.3	5	LINE
Site 1	0.0.0.0	1-2	15454-OPT-PRE	4	LINE-2-2-TX	DC-TX		1-2	15454-OPT-PRE	3	LINE
Site 1	0.0.0.0	1-17	15454-OSC-CSM	1	LINE-17-1-RX	COM-RX		1-15	15454-AD-1C-30.3	6	LINE-
Site 1	0.0.0.0	1-17	15454-OSC-CSM	2	LINE-17-1-TX	COM-TX		1-16	15454-OPT-PRE	1	LINE-
Site 1	0.0.0.0	1-16	15454-OPT-PRE	2	LINE-16-1-TX	COM-TX		1-15	15454-AD-1C-30.3	5	LINE-
Site 1	0.0.0.0	1-16	15454-OPT-PRE	4	LINE-16-2-TX	DC-TX		1-16	15454-OPT-PRE	3	LINE-
Site 1	0.0.0.0	1-1	15454-OSC-CSM	1	LINE-1-1-RX	COM-RX		1-3	15454-AD-1C-30.3	6	LINE
Site 1	0.0.0.0	1-3	15454-AD-1C-30.3	3	LINE-3-1-RX	EXP-RX		1-15	15454-AD-1C-30.3	4	LINE-
Site 1	0.0.0.0	1-3	15454-AD-1C-30.3	4	LINE-3-1-TX	EXP-TX		1-15	15454-AD-1C-30.3	3	LINE-
Site 1	0.0.0.0	1-3	15454-AD-1C-30.3	1	CHAN-3-1-RX	30.3-RX		1-4	15454-10T-L1-30.3	2	CHAN-
Site 1	0.0.0.0	1-3	15454-AD-1C-30.3	2	CHAN-3-1-TX	30.3-TX		1-4	15454-10T-L1-30.3	2	CHAN-
Site 1	0.0.0.0	1-15	15454-AD-1C-30.3	1	CHAN-15-1-RX	30.3-RX		1-14	15454-10T-L1-30.3	2	CHAN-
Site 1	0.0.0.0	1-15	15454-AD-1C-30.3	2	CHAN-15-1-TX	30.3-TX		1-14	15454-10T-L1-30.3	2	CHAN-

Step 2 Export the internal connections table:

a. Click **Export**.

b. Enter a file name in the File Name field of the Save Table dialog box.

c. In the Files of Type field, choose HTML.

d. Click **Save**.

Step 3 Open the exported MetroPlanner internal connections file in a web browser, and then print the file.

Step 4 Connect the cables to the slot and ports specified in the printed MetroPlanner internal connections file. Use the following tasks as a general guide for connecting the DWDM cables. However, connect the cables to the slot and port specified in the MetroPlanner internal connections file.

- DLP-A424 Install Fiber-Optic Cables for a Terminal Node, page 2-44
- DLP-A425 Install Fiber-Optic Cables for a Hub Node, page 2-45
- DLP-A426 Install Fiber-Optic Cables for a Line Amplifier Node, page 2-47
- DLP-A427 Install Fiber-Optic Cables for an Amplified or Passive OADM Node, page 2-50

Step 5 If 32DMX-O or 32MUX-O cards are installed, connect them to the patch panel above the ONS 15454 shelf.

Step 6 Connect DWDM cards to the 32DMX-O or 32MUX-O cards through the patch panel above the ONS 15454 shelf.

Step 7 If TXP, MXP, or OC-N line cards are installed, connect each card with the correct DWDM card according to your site plan. OC-N line connections are not shown in MetroPlanner.

Step 8 Return to your originating procedure (NTP).

DLP-A396 Calculate DWDM Connections

Purpose	This task calculates the ONS 15454 cable connections for ONS 15454s provisioned for DWDM or DWDM and TDM (hybrid).
Tools/Equipment	None
Prerequisite Procedures	A DWDM network plan calculated by Cisco MetroPlanner. DLP-A389 Connect the Internal DWDM Cables, page 5-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **WDM-ANS** > **Connections** tabs.

Step 2 Click the **Calculate Connections** button.

Step 3 Create any connections that require manual provisioning (indicated by a "Yes" in the MetroPlanner connections file Manually Set column). See the "DLP-A406 Create a DWDM Connection" task on page 5-8.

Step 4 Verify that the connections in the CTC Connections tab match the connections in the MetroPlanner internal connections file. (The CTC Connections tab will not show connections between TXP, MXP, and OC-N line cards and DWDM cards.) If connections are not correct:

a. Delete the connection. See the "DLP-A405 Delete a DWDM Connection" task on page 5-9.

b. Uninstall the fibers from the incorrect slot/card/port.

c. Connect the fiber to the correct slot/card/port, then repeat Step 2.

Step 5 Return to your originating procedure (NTP).

DLP-A406 Create a DWDM Connection

Purpose	This task creates a DWDM connection.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Connections** tabs.

Step 2 Click the **Create** button.

Step 3 In the Create Optical Link dialog box, choose the From and To slots and ports from the drop-down menus.

Step 4 If the connection is unidirectional, uncheck the **bidirectional** check box.

Step 5 Click **OK**. The new connection appears in the Connections table, but its State is "Uncommitted."

Step 6 Click the new connection in the table. Click the **Commit** button. The connection state changes to "Connected."

Step 7 Return to your originating procedure (NTP).

DLP-A405 Delete a DWDM Connection

Purpose	This task deletes a DWDM connection.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Connection** tabs.

Step 2 Click the connection you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

NTP-A270 Run Automatic Node Setup

Purpose	This procedure launches the DWDM Automatic Node Setup (ANS) function. ANS adjusts the values of the variable optical attenuators (VOAs) to equalize the per-channel power at the amplifier level.
Tools/Equipment	None
Prerequisite Procedures	An Installation Parameters file for the node exported from Cisco MetroPlanner. NTP-A269 Provision the DWDM Connections, page 5-5
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 3 Complete the "DLP-A400 Import a Cisco MetroPlanner Configuration File" task on page 5-10.

Step 4 Complete the "DLP-A396 Calculate DWDM Connections" task on page 5-8.

Step 5 In node view, click the **Provisioning** > **WDM-ANS** > **Port Status** tabs.

Step 6 Click **Launch ANS**.

Step 7 In the Apply Launch ANS dialog box, click **Yes**. Automatic Node Setup (ANS) adjusts the values of the variable optical attenuators (VOAs) to equalize the per-channel power at the amplifier level.

Step 8 In the Launch ANS confirmation dialog box, click **OK**.

Step 9 Verify that the Link Status column displays a "Regulated" status for all ports. If any links say Not Regulated, repeat the "NTP-A269 Provision the DWDM Connections" procedure on page 5-5 to verify that all connections have been provisioned correctly, paying attention to connections that require manual provisioning.

Step 10 Complete the "DLP-A342 Provision OSC Terminations" task on page 5-11.

Step 11 If the node timing is line timing with an OSCM or OSC-CSM card as a timing reference, complete the "NTP-A28 Set Up Timing" task on page 4-22.

Stop. **You have completed this procedure**.

DLP-A400 Import a Cisco MetroPlanner Configuration File

Purpose	This task imports a Cisco MetroPlanner configuration file into the node to configure the node automatically.
Tools/Equipment	None
Prerequisite Procedures	A Cisco MetroPlanner network configuration file must be located on an available local or network drive. DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Export the Installation Parameters for your node from Cisco MetroPlanner. If the parameters file has been exported, continue with Step 2.

a. In MetroPlanner, right-click the node icon and choose **Site Installation** > **Assisted Conf Setup**.

b. In the dialog box, choose a location to save the MetroPlanner installation file.

Step 2 In CTC node view, click the **Provisioning > WDM-ANS > NE Update** tabs.

Step 3 Click **Import**.

Step 4 In the Import Defaults From File dialog box, enter the path to the configuration file, or click **Browse** and navigate to the configuration file using the Open dialog box.

Step 5 Click **OK**.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A342 Provision OSC Terminations

Purpose	This task creates the DWDM OSC terminations required for network setup of a system that includes ONS 15454 DWDM optical filters and amplifiers.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

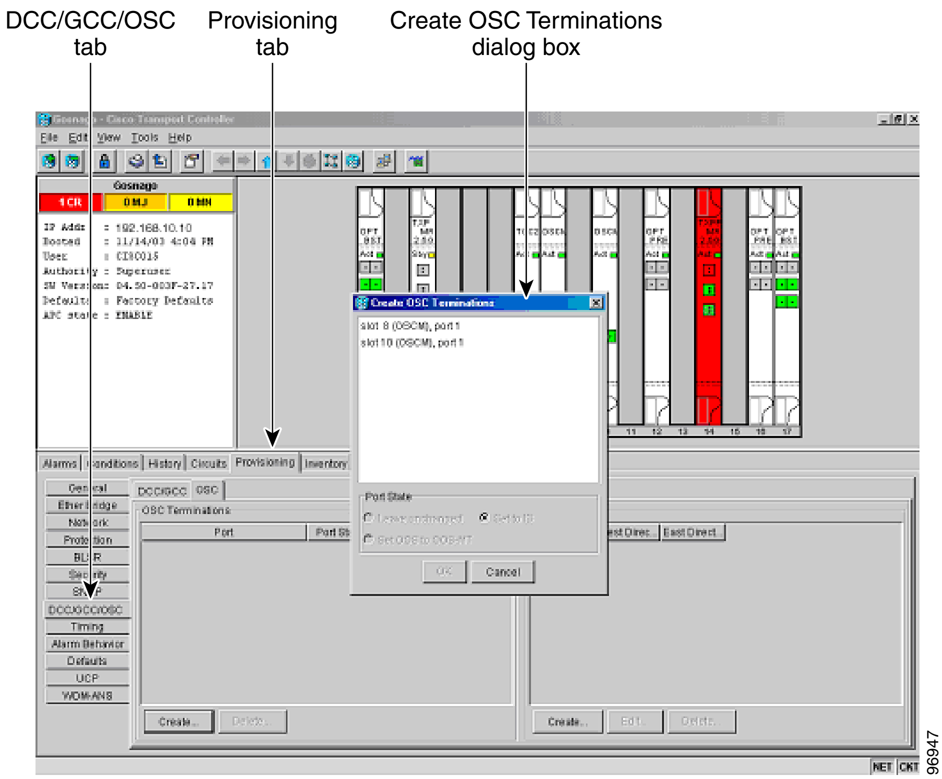
Step 1 In node view click the **Provisioning > WDM-ANS > Connections** tabs.

Step 2 Click **Calculate Connections**. Ports that can have an OSC termination appear.

Step 3 Click the **Provisioning > DCC/GCC/OSC > OSC** tabs.

Step 4 In the OSC Terminations pane, click **Create (Figure 5-3).**

Figure 5-3 OSC Terminations Pane



Step 5 In the Create OSC Terminations dialog box, click the ports where you want to create the OSC termination. To select more than one port, press the **Shift** key or the **Ctrl** key.

Note OSC on the DWDM node uses a separate OC3 channel to transport the section data communications channel (SDCC), which is used for ONS 15454 DCC terminations.

Step 6 Click **OK**. Ports are automatically placed in service. Until all network OSC terminations are created and the ports are in service, the following alarms might appear: EOC (SDCC Termination Failure) and power failure alarms on the OPT-BST or OSC-CSM, such as Loss of Continuity alarms.

Step 7 Return to your originating procedure (NTP).

NTP-A271 Verify OSCM and OSC-CSM Transmit Power

Purpose	This procedure verifies the transmit power of the ONS 15454 Optical Service Channel Module (OSCM) and the Optical Service Channel + Combiner Separator Module (OSC-CSM).
Tools/Equipment	None
Prerequisite Procedures	NTP-A270 Run Automatic Node Setup, page 5-9
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 In the node view shelf graphic, double-click the OSCM or OSC-CSM card in Slot 8.

Step 3 Click the **Maintenance** tab.

Step 4 Verify that the ALS Command is set to OSRI off.

Step 5 From the ALS Mode drop-down menu, choose **Disable**. Click **Apply**.

Step 6 Click the **Provisioning > Optical Line** tabs.

Step 7 For the TX (transmit) port entry, verify that the value in the Power column falls within the following ranges:

- For OSCM cards installed on nodes set to Control Gain, the power should be –5 dBm.
- For OSC-CSM card installed on nodes set to Control Gain, the power should be a minimum of –6 dBm on OADM nodes.
- For OSC-CSM cards installed on nodes configured as a passive or active OADM nodes, the power level depends on the Pout OADM Stage power level on the WDM-ANS > Provisioning tab:
  - If the Pout OADM Stage value is less than –6.5 dBm +/– 0.5 dBm, the OSC-CSM power should be equal to that power.
  - If the Pout OADM Stage value is greater than –6.5 dBm +/– 0.5 dBm, the OSC-CSM power should be –6.5 dBm +/– 0.5 dBm.
- For OSC-CSM cards installed on hybrid nodes, the Pout-osc should be:
  - –5.0 dBm if the DWDM system type is Control Gain and
  - –1.5 dBm if the DWDM system type is Control Power.

Step 8 If the OSCM or OSC-CSM power levels are not within the ranges specified in Step 7, complete the following steps. Otherwise, continue with Step 9.

a. Click the **Maintenance > ALS** tabs. Verify that OSRI is set to off and ALS Mode is set to Disable.

b. Clean the optical connections. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21.

c. Verify the optical connections inside the unit.

d. Relaunch ANS.

Step 9 Click the **Maintenance** tab.

Step 10 From the ALS Mode drop-down menu, choose **Automatic Restart**. Click **Apply**.

Step 11 Continue with the "NTP-A273 Terminal and Hub Node Acceptance Test" procedure on page 5-13.

Stop. **You have completed this procedure**.

NTP-A273 Terminal and Hub Node Acceptance Test

Purpose	This procedure tests a DWDM terminal or hub node.
Tools/Equipment	None
Prerequisite Procedures	Tunable laser or TXP, MXP, or OC-N line cards must be installed.
	#2 Bulk attenuators (10 dB)
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 4 In node view, click the **Provisioning** > **WDM-ANS** > **Port Status** tabs. Verify that all links have a Regulated status. If any links say Not Regulated, click **Launch ANS**.

Step 5 On one side of the node, either east or west (if the node is a terminal, the terminal side), create a physical loop back on the OPT BST by using a patch cord with 10 dB bulk attenuators to connect the card's Line-TX port with Line-RX port.

Step 6 On the OSCM card, verify that the OSC link becomes active. (OSC Termination must already be provisioned, see the "DLP-A342 Provision OSC Terminations" task on page 5-11.)

Note The OSC signal loop back might cause an SDCC Termination Failure alarm.

Step 7 Tune the tunable laser on the first wavelength (1530.33 nm) of the 100Ghz ITU-T grid and connect it to the CHAN RX 01 port on the 32 MUX-O card using the available patch-panel.

Step 8 Double-click the west or east 32 MUX-O card on the shelf graphic to open card view.

Step 9 Click the **Provisioning** > **Optical Chn** > **Parameters** tabs.

Step 10 Set the port #1 status to **OOS_MT.** This puts the port Out Of Service, but enables VOA provisioning.

Step 11 Verify that the Port 1 power level reaches the provisioned set point (VOA Power Ref).

> **Note** Output power that is lower than the specified value might keep the 32 MUX-O card from reaching the provisioned set point.

Step 12 Verify that the west or east OPT BST card is working properly:

a. In node view, double-click the west or east OPT-BST card to open card view.

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

c. Verify that the laser status is set to On. If so, continue with Step 13. If not, continue with Substep d.

d. Verify that the ALS Command is set to OSRI Off (optical safety remote interlock is not enabled).

e. If the ALS Command is set to OSRI On, choose **OSRI Off**. Click **Apply**.

f. Check the Laser Status. If it is not set to On, replace the card. See the "NTP-A242 Install the DWDM Cards" procedure on page 2-25.

> **Note** On Provisioning > Opt.Ampli.Line> Parameters tab, the power value on port #6 reaches the provisioned set point = +2 dBm. However, the actual value reported by CTC also includes the ASE power contribution, so the value is always greater than +2 dBm (Power Ref).

> **Note** When Laser Status is off, the Port #2 power is lower than or equal to –1 dBm as shown. This value is not a significant optical power and must be ignored.

Step 13 Verify that the west or east OPT-PRE card is working properly:

a. Display the west or east OPT-PRE card in card view (double-click the card on the shelf graphic).

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

c. Verify that the Laser Status is ON.

> **Note** On Provisioning > Opt.Ampli.Line > Parameters tab, the power value on port #6 reaches the provisioned set point = +2 dBm. However, the actual value reported by CTC also includes the ASE power contribution, so the value is always greater than +2 dBm (Power Ref).

d. Click the **Provisioning > Optical Line > Parameters** tabs.

e. Verify that the DCU IL (insertion loss) value is less than or equal to 10 dB.

> **Note** When Laser Status is off, the Port #2 power is lower or equal to –1 dBm is shown. This value is not a significant optical power and must be ignored.

Step 14 Verify the west or east 32 DMX-O in card view:

a. Display the east or west 32 DMX-O card in card view.

b. Click the **Provisioning > Optical Chn > Parameters** tabs,

c. Set the status of port #1 to **OOS_MT**.

d. Check that the Power value on part #1 reaches the provisioned set point (VOA Power Ref).

e. (*optional*) Connect a power meter to the CHAN TX 01 port through the patch-panel. Verify that the physical optical power value coming out of drop port #1 on the west 32 DMX-O card is consistent with the value read (the maximum allowed error is +/–0.5 dBm).

Step 15 Restore the default OOS status on the 32 MUX-O card port that was set to OOS_MT in Step 10.

Step 16 Restore the default OOS status on the 32 DMX-O card port that was set to OOS_MT in Step 14.

Step 17 Launch ANS to restore the correct node configuration.

Step 18 Repeat Steps 7 through 17 for the remaining 32 wavelengths of the 100 Ghz grid to verify the correct behavior of all VOAs inside the 32 MUX-O and 32 DMX-O cards.

Step 19 If the node is a hub node, repeat Steps 5 through 18. If it is a terminal node, continue with Step 20.

Step 20 Remove the loopbacks.

Step 21 Restore the default OOS status on all ports previously set to OOS_MT and launch ANS to recover the correct node configuration.

Step 22 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 23 Continue with the "NTP-A272 View DWDM Node Parameters" procedure on page 5-15.

Stop. **You have completed this procedure**.

NTP-A272 View DWDM Node Parameters

Purpose	This procedure allows you to view and manually change DWDM parameters on the ONS 15454 after it is provisioned for DWDM.
Tools/Equipment	None
Prerequisite Procedures	NTP-A271 Verify OSCM and OSC-CSM Transmit Power, page 5-12
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution Manually changing parameters that have been calculated by Cisco MetroPlanner is not recommended.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to view the DWDM parameters. If you are already logged in, continue with Step 2.

Step 2 Perform one of the following tasks:

- DLP-A401 View DWDM Hub Node Settings, page 5-16.
- DLP-A402 View DWDM Terminal Node Settings, page 5-18.

- DLP-A403 View DWDM OADM Node Settings, page 5-19.
- DLP-A404 View DWDM Line Node Settings, page 5-21.

Stop. **You have completed this procedure**.

DLP-A401 View DWDM Hub Node Settings

Purpose	This task enables you to view and manually change DWDM hub node parameters including the network type, system types, network power levels, and channel power levels for a DWDM hub node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 View the information shown in Table 5-2. In the table, the West Side of the node is equipped with cards that receive from the west and transmit to the east. The East Side of the node is equipped with cards that receive from the east and transmit to the west.

Table 5-2 DWDM Hub Node Settings

Parameter	Description	Default Value	Options
Network type	Defines the DWDM network type.	Metro-Core	Metro-Core—Channels are equalized Metro-Access—Channels are not equalized to minimize the number of amplifiers in the ring
West Side			
System Type	Defines the west-side DWDM fiber type, number of channels, and control mode. Table 5-3 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
Pdrop	Sets the west-side expected drop power level on the client interface. Pdrop is the power level of each channel after it is demultiplexed. The power is then sent to the client.	–14 dBm	–50 dBm to 30 dBm
Pexpress	Sets the west-side expected per-channel power on the pass-through interface.	–12 dBm	–50 dBm to 30 dBm

Table 5-2 DWDM Hub Node Settings (continued)

Parameter	Description	Default Value	Options
Pout-mux Stage	Sets the per-channel output power at the multiplexing stage. Pout-mux is the power that is sent to the multiplexer after the power from the client transmitters is gathered. The VOAs keep the power sent to the multiplexer at a constant level.	–18 dBm	–50 dBm to 30 dBm
East Side			
System Type	Defines the east-side DWDM fiber type, number of channels, and control mode. Table 5-3 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
Pdrop	Sets the east-side expected drop power level on the client interface. Pdrop is the power level of each channel after it is demultiplexed. The power is then sent to the client.	–14 dBm	–50 dBm to 30 dBm
Pexpress	Sets the east-side expected per-channel power on the pass-through interface.	–12 dBm	–50 dBm to 30 dBm
Pout-mux Stage	Sets the per-channel output power at the multiplexing stage. Pout-mux is the power that is sent to the multiplexer after the power from the client transmitters is gathered. The VOAs keep the power sent to the multiplexer at a constant level.	–18 dBm	–50 dBm to 30 dBm

Table 5-3 shows the system types that can be assigned to the node.

Table 5-3 DWDM System Types

System Type	Per-Channel Power	Control Mode
SMF-28 32 Ch Control Gain	2 dBm	Control gain
SMF-28 32 Ch Control Power	2 dBm	Control power
SMF-28 8 Ch Control Power	8 dBm	Control power
SMF-28 16 Ch Control Power	5 dBm	Control power

Step 3 Return to your originating procedure (NTP).

DLP-A402 View DWDM Terminal Node Settings

Purpose	This task enables you to view and manually change DWDM terminal node parameters including its network type, system types, network power levels, and channel power levels.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 View the fields shown in Table 5-4. In the table, the West Side of the node is equipped with cards that receive from the west and transmit to the east. The East Side of the node is equipped with cards that receive from the east and transmit to the west. The fields that appear depend on the terminal node type.

Table 5-4 DWDM Terminal Node Settings

Parameter	Description	Default Value	Options
Network type	Defines the DWDM network type.	Metro-Core	Metro-Core—Channels are equalized. Metro-Access—Channels are not equalized to minimize the number of amplifiers in the ring.
Term West Side/ East Side			
System Type	Defines the west-side DWDM system type (fiber type, number of channels, control mode). Table 5-3 on page 5-17 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
Pdrop	Sets the expected drop power level on the client interface. Pdrop is the power level of each channel after it is demultiplexed. The power is then sent to the client.	–14 dBm/	–50 dBm to 30 dBm
Pout-mux Stage	Sets the per-channel output power at the multiplexing stage. Pout-mux is the power that is sent to the multiplexer after the power from the client transmitters is gathered. The VOAs keep the power sent to the multiplexer at a constant level.	–18 dBm/	–50 dBm to 30 dBm

Step 3 Return to your originating procedure (NTP).

DLP-A403 View DWDM OADM Node Settings

Purpose	This task enables you to view and manually change DWDM add/drop multiplexing node parameters including its network type, system types, network power levels, and channel power levels.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 View the fields shown in Table 5-5. In the table, the West Side of the node is equipped with cards that receive from the west and transmit to the east. The East Side of the node is equipped with cards that receive from the east and transmit to the west.

Table 5-5 DWDM OADM Node Settings

Parameter	Description	Default Value	Options
Network type	Defines the DWDM network type.	Metro-Core	Metro-Core—Channels are equalized. Metro-Access—Channels are not equalized to minimize the number of amplifiers in the ring.
West Side			
System Type	Defines the west-side DWDM system type. Table 5-3 on page 5-17 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
Pout-oadm Stage	Sets the west-side per-channel output power at the OADM stage.	+2 dBm	–50 dBm to 30 dBm
Pin-oadm Stage	Sets the west-side per-channel input power at the OADM stage.	–14 dBm	–50 dBm to 30 dBm
Pout Band [*nn.n*]	Sets the west-side per-band output power for a specific drop band, where *nn.n* is the channel ID. Up to 8 bands might appear, 30.3, 34.2, 38.1, 42.1, 46.1, 50.1, 54.1, and 58.1, depending on the optical filter cards that are installed in the node.	–14 dBm	–50 dBm to 30 dBm

Table 5-5 DWDM OADM Node Settings (continued)

Parameter	Description	Default Value	Options
East Side			
System Type	Defines the east-side DWDM system type. Table 5-3 on page 5-17 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
Pout-oadm Stage	Sets the east-side per-channel power out from the OADM stage.	+2 dBm	–50 dBm to 30 dBm
Pin-oadm Stage	Sets the east-side per-channel input power from the OADM stage.	–14 dBm	–50 dBm to 30 dBm
Pout Band [*nn.n*]	Sets the east-side per-band power for a specific drop band, where *nn.n* is the channel ID. Up to 8 bands might appear, 30.3, 34.2, 38.1, 42.1, 46.1, 50.1, 54.1, and 58.1, depending on the optical filter cards that are installed in the node.	–14 dBm	–50 dBm to 30 dBm

Table 5-6 shows the OADM channels.

Table 5-6 OADM Channels

Channel No.	Channel ID	Frequency (GHz)	Wavelength (nm)
1	30.3	195.9	1530.33
2	31.2	195.8	1531.12
3	31.9	195.7	1531.90
4	32.6	195.6	1532.68
5	34.2	195.4	1534.25
6	35.0	195.3	1535.04
7	35.8	195.2	1535.82
8	36.6	195.1	1536.61
9	38.1	194.9	1538.19
10	38.9	194.8	1538.98
11	39.7	194.7	1539.77
12	40.5	194.6	1540.56
13	42.1	194.4	1542.14
14	42.9	194.3	1542.94
15	43.7	194.2	1543.73
16	44.5	194.1	1544.53
17	46.1	193.9	1546.12

Table 5-6 OADM Channels (continued)

Channel No.	Channel ID	Frequency (GHz)	Wavelength (nm)
18	46.9	193.8	1546.92
19	47.7	193.7	1547.72
20	48.5	193.6	1548.51
21	50.1	193.4	1550.12
22	50.9	193.3	1550.92
23	51.7	193.2	1551.72
24	52.5	193.1	1552.52
25	54.1	192.9	1554.13
26	54.9	192.8	1544.94
27	55.7	192.7	1555.75
28	56.5	192.6	1556.55
29	58.1	192.4	1558.17
30	58.9	192.3	1558.98
31	59.7	192.2	1559.79
32	60.6	192.1	1560.61

Step 3 Return to your originating procedure (NTP).

DLP-A404 View DWDM Line Node Settings

Purpose	This task enables you to view and manually change DWDM line node parameters, including its network and system types.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 View the fields shown in Table 5-7. In the table, the West Side of the node is equipped with cards that receive from the west and transmit to the east. The East Side of the node is equipped with cards that receive from the east and transmit to the west.

Table 5-7 DWDM Line Node Settings

Parameter	Description	Options
Network type	Defines the DWDM network type.	Metro-Core—Channels are equalized Metro-Access—Channels are not equalized to minimize the number of amplifiers in the ring
West Side		
System Type	Defines the west-side DWDM system type. Table 5-3 on page 5-17 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power
East Side		
System Type	Defines the east-side DWDM system type. Table 5-3 on page 5-17 shows the per-channel power and control mode for each system type.	SMF-28 32 Ch Control Gain SMF-28 32 Ch Control Power SMF-28 8 Ch Control Power SMF-28 16 Ch Control Power

Step 3 Return to your originating procedure (NTP).

DLP-A331 View DWDM NE Update Parameters

Purpose	Use this task to view all DWDM parameters that have been imported into the node from Cisco MetroPlanner.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > NE Update** tabs.

Step 2 View the parameters shown in Table 5-8.

Table 5-8 NE Update Parameters

Parameter Name	General Name	Min dBm	Max dBm	Default
dwdm.common.NetworkType1	Network Type	[1]	1	Metro-Core
dwdm.common.SystemTypeValueW	System Type West	0	3	0
dwdm.common.SystemTypeValueE	System Type East	0	3	0
dwdm.common.OscLosThW	OSC LOS Threshold West	-50	+30	-2 (OPT-BST) -40 (OSC-CSM)
dwdm.common.OscLosThE	OSC LOS Threshold East	-50	+30	-2 (OPT-BST) -40 (OSC-CSM)
dwdm.common.ChLosThW	Channel LOS Threshold West	-50	+30	+10 (OPT-BST) -30 (OSC-CSM)
dwdm.common.ChLosThE	Channel LOS Threshold East	-50	+30	+10 (OPT-BST) -30 (OSC-CSM)
dwdm.hub_site.power.DropW	Hub – Drop Power West	-50	+30	-14
dwdm.hub_site.power.DropE	Hub – Drop Power East	-50	+30	-14
dwdm.hub_site.power.ExpressW	Hub – Express Power West	-50	+30	-14
dwdm.hub_site.power.ExpressE	Hub – Express Power East	-50	+30	-14
dwdm.hub_site.power.OutMuxW	Hub – Mux Output Power West	-50	+30	-14
dwdm.hub_site.power.OutMuxE	Hub – Mux Output Power East	-50	+30	-14
dwdm.oadm_site.power.OutOadmW	OADM – Output Power West	-50	+30	-14
dwdm.oadm_site.power.OutOadmE	OADM – Output Power East	-50	+30	-14
dwdm.oadm_site.power.InOadmW	OADM – Input Power West	-50	+30	-14
dwdm.oadm_site.power.InOadmE	OADM – Input Power East	-50	+30	-14
dwdm.oadm_site.power.DropB1W	OADM – Band 1 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB1E	OADM – Band 1 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB2W	OADM – Band 2 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB2E	OADM – Band 2 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB3W	OADM – Band 3 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB3E	OADM – Band 3 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB4W	OADM – Band 4 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB4E	OADM – Band 4 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB5W	OADM – Band 5 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB5E	OADM – Band 5 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB6W	OADM – Band 6 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB6E	OADM – Band 6 Drop Power East	-50	+30	-14
dwdm.oadm_site.power.DropB7W	OADM – Band 7 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB7E	OADM – Band 7 Drop Power East	-50	+30	-14

Table 5-8 NE Update Parameters (continued)

Parameter Name	General Name	Min dBm	Max dBm	Default
dwdm.oadm_site.power.DropB8W	OADM – Band 8 Drop Power West	-50	+30	-14
dwdm.oadm_site.power.DropB8E	OADM – Band 8 Drop Power East	-50	+30	-14

1. Three network types are available: Metro-Core, Metro-Access, and Not-DWDM.

Step 3 Return to your originating procedure (NTP).

CHAPTER 6

Turn Up Network

This chapter explains how to turn up and test Cisco ONS 15454 networks, including point-to-point networks, linear add-drop multiplexers (ADMs), path protection, and bidirectional line switched rings (BLSRs).

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.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A35 Verify Node Turn Up, page 6-2—Complete this procedure before beginning network turn up.
2. NTP-A124 Provision a Point-to-Point Network, page 6-3—Complete as needed.
3. NTP-A173 Point-to-Point Network Acceptance Test, page 6-7—Complete this procedure after you provision a point-to-point network.
4. NTP-A38 Provision a Linear ADM Network, page 6-12—Complete as needed.
5. NTP-A174 Linear ADM Network Acceptance Test, page 6-13—Complete this procedure after you provision a linear ADM.
6. NTP-A40 Provision BLSR Nodes, page 6-15—Complete this procedure to provision ONS 15454s in a two-fiber or four-fiber bidirectional line switched ring (BLSR).
7. NTP-A126 Create a BLSR, page 6-18—Complete this procedure after you provision the BLSR nodes.
8. NTP-A175 Two-Fiber BLSR Acceptance Test, page 6-22—Complete this procedure after you create a two-fiber BLSR.
9. NTP-A176 Four-Fiber BLSR Acceptance Test, page 6-30—Complete this procedure after you create a four-fiber BLSR.
10. NTP-A44 Provision Path Protection Nodes, page 6-36—Complete as needed.
11. NTP-A177 Path Protection Acceptance Test, page 6-38—Complete this procedure after you create a path protection.

12. NTP-A216 Provision a Traditional Path Protection Dual Ring Interconnect, page 6-41—As needed, complete this procedure after you provision a path protection.
13. NTP-A217 Provision an Integrated Path Protection Dual Ring Interconnect, page 6-43—As needed, complete this procedure after you provision a path protection.
14. NTP-A224 Provision an Open-Ended Path Protection, page 6-44—As needed, complete this procedure after you provision a path protection.
15. NTP-A225 Open-Ended Path Protection Acceptance Test, page 6-46—As needed, complete this procedure after you provision an open-ended path protection.
16. NTP-A46 Subtend a Path Protection from a BLSR, page 6-49—Complete as needed.
17. NTP-A47 Subtend a BLSR from a Path Protection, page 6-50—Complete as needed.
18. NTP-A48 Subtend a BLSR from a BLSR, page 6-51—Complete as needed.
19. NTP-A172 Create a Logical Network Map, page 6-52—Complete as needed.

NTP-A35 Verify Node Turn Up

Purpose	This procedure verifies that an ONS 15454 is ready for network turn up before adding it to a network.
Tools/Equipment	None
Prerequisite Procedures	Chapter 4, "Turn Up Node"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on the network you will test. If you are already logged in, continue with Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 3 Verify that the SW Version and Defaults shown in the node view status area match the software version and NE defaults shown in your site plan. If either is not correct, complete the following procedures as needed:

- If the software is not the correct version, install the correct version from the ONS 15454 software CD. Upgrade procedures are located in the *Cisco ONS 15454 Upgrade Guide*. Follow the upgrade procedures appropriate to the software currently installed on the node. TCC2 cards can also be ordered with the latest software release.
- If the node defaults are not correct, import the network element defaults. Refer to the *Cisco ONS 15454 Network Element Defaults* for Software R4.6.

Step 4 Click the **Provisioning > General** tabs. Verify that all general node information settings match the settings of your site plan. If not, see the "NTP-A81 Change Node Management Information" procedure on page 12-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that timing settings match the settings of your site plan. If not, see the "NTP-A85 Change Node Timing" procedure on page 12-23.

Step 6 Click the **Provisioning > Network** tabs. Ensure that the IP settings and other CTC network access information is correct. If not, see the "NTP-A201 Change CTC Network Access" procedure on page 12-4.

Step 7 Click the **Provisioning > Protection** tabs. Verify that all protection groups have been created according to your site plan. If not, see the "NTP-A203 Modify or Delete Card Protection Settings" procedure on page 12-15.

Step 8 Click the **Provisioning > Security** tabs. Verify that all users have been created and their security levels and policies match the settings indicated by your site plan. If not, see the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 9 If SNMP is provisioned on the node, click the **Provisioning > SNMP** tabs. Verify that all SNMP settings match the settings of your site plan. If not, see the "NTP-A87 Change SNMP Settings" procedure on page 12-33.

Step 10 Provision the network using the applicable procedure shown in the "Before You Begin" section on page 6-1.

Stop. You have completed this procedure.

NTP-A124 Provision a Point-to-Point Network

Purpose	This procedure provisions two ONS 15454s in a point-to-point (terminal) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on an ONS 15454 in the network where you want to provision a point-to-point configuration. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards. Complete the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 if protection has not been created.

Step 3 Repeat Steps 1 and 2 for the second point-to-point node.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, verify that the working card in one node connects to the working card in the other node, and that the protect card in one node connects to the protect card in the other node.

Step 5 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for the working OC-N port on both point-to-point nodes.

Note DCC terminations are not provisioned on the protect ports.

Note If the point-to-point nodes are not connected to a LAN, you will need to create the DCC terminations using a direct (craft) connection to the node. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 6 Complete the "DLP-A214 Change the Service State for a Port" task on page 6-6 to put the protect card in-service.

Step 7 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-A28 Set Up Timing" procedure on page 4-22 for one or both of the nodes. If a node uses line timing, make its working OC-N card the timing source. The system will automatically choose the corresponding protect OC-N card the protect timing source. This will be visible in the Maintenance > Timing tab.

Step 8 Complete the "NTP-A173 Point-to-Point Network Acceptance Test" procedure on page 6-7.

Stop. You have completed this procedure.

DLP-A354 Provision SONET DCC Terminations

Purpose	This task creates the SONET Data Communications Channel terminations required for alarms, administration data, signal control information, and messages.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When SDCC is provisioned, an LDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

Step 1 In node view, click the **Provisioning > DCC/GCC/OSC > SDCC** tabs.

Step 2 Click **Create.**

Step 3 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 or the Ctrl key.

Note SDCC refers to the Section DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the "DLP-A313 Create a DCC Tunnel" task on page 8-93.

Step 4 In the Port State area, click the **Set to IS** radio button.

Step 5 Verify that the Disable OSPF on DCC Link check box is unchecked.

Step 6 Click **OK**.

> **Note** EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

Step 7 Return to your originating procedure (NTP).

DLP-A355 Provision SONET LDCC Terminations

Purpose	This task creates the SONET Line Data Communications Channel terminations used for tunneling third-party vendor equipment communications through a Cisco ONS 15454 network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

> **Note** When LDCC is provisioned, an SDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

Step 1 In node view, click the **Provisioning > DCC/GCC/OSC > LDCC** tabs.

Step 2 Click **Create.**

Step 3 In the Create LDCC Terminations dialog box click the ports where you want to create the LDCC termination. To select more than one port, press the Shift key or the Ctrl key.

> **Note** LDCC refers to the Line DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the "DLP-A313 Create a DCC Tunnel" task on page 8-93.

Step 4 In the Port State area, click the **Set to IS** radio button.

Step 5 Verify that the Disable OSPF on DCC Link check box is unchecked.

Step 6 Click **OK**.

> **Note** EOC-L (Line DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

Step 7 Return to your originating procedure (NTP).

DLP-A214 Change the Service State for a Port

Purpose	This task puts a port in service or removes a port from service.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To provision Ethernet ports, see the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66 or the "DLP-A222 Provision G-Series Ethernet Ports" task on page 8-86.

Step 1 In node view on the shelf graphic, double-click the card with the port(s) you want to put in or out of service. The card view appears.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 In the State area, choose one of the following:

- **IS**—The port is in-service.
- **OOS**—The port is out-of-service. Traffic is not passed on the port until the service state is changed to IS, OOS_MT, or OOS_AINS.
- **OOS_MT**—The port is in a maintenance state. The maintenance state does not interrupt traffic flow, but alarm reporting is suppressed and loopbacks are allowed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use OOS_MT for testing or to suppress alarms temporarily. Change the state to IS, OOS, or OOS_AINS when testing is complete.
- **OOS_AINS**—The port is in an auto-inservice state; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to IS. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

Step 4 If you set State to OOS-AINS, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in OOS-AINS after a signal is continuously received. When the soak period elapses, the port changes to IS.

Step 5 Click **Apply**.

Step 6 As needed, repeat this task for each port.

Step 7 Return to your originating procedure (NTP).

NTP-A173 Point-to-Point Network Acceptance Test

Purpose	This procedure tests a point-to-point network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 6-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the point-to-point nodes. The node (default) view appears. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export alarm data.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the condition information.

Step 5 On the network map, double-click a point-to-point node to open it in node view.

Step 6 Create a test circuit from the login node to the other point-to-point node:

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface to the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS3. Next, choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector the other to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step 9.

Step 9 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's transmit (Tx) connector; attach the other end to the port's receive (Rx) connector.

Step 10 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the receive (Rx) connector on the circuit source card.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector on the circuit source card.

Step 11 Verify that the test set has a clean signal. If a clean signal is not present, repeat Steps 6 through 10 to make sure the test set and cabling are configured correctly.

Step 12 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 13 Inject BIT errors from the test set. Verify that the errors appear at the test set, indicating a complete end-to-end circuit.

Step 14 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 15 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Step 16 Complete the "DLP-A88 Optical 1+1 Protection Test" task on page 6-11.

Step 17 Set up and complete a BER Test. Use the existing configuration and follow your site requirements for the specified length of time. Record the test results and configuration.

Step 18 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 19 From the View menu, choose **Go to Network View**.

Step 20 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarms information.

Step 21 Repeat Steps 9 through 20 for the other point-to-point node.

Step 22 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 23 Delete the test circuit. See the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

Stop. You have completed this procedure.

DLP-A356 TCC2 Active/Standby Switch Test

Purpose	This task verifies that the TCC2 cards can effectively switch from one to another.
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the TCC2 cards you are testing to open it in node view.

Step 5 Make a note of which TCC2 is active and which is standby by examining the LEDs on the shelf graphic. TCC2 cards are installed in Slot 7 and Slot 11. The active TCC2 has a green ACT LED, and the standby TCC2 has an amber SBY LED.

Step 6 On the shelf graphic, right-click the active TCC2 and choose **Reset** from the shortcut menu.

Step 7 In the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message appears.

Step 8 Click **OK**. On the network view map, the node where you reset the TCC2 will be gray.

Step 9 After the node icon turns green (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby TCC2 has a green ACT LED.
- The previous active TCC2 LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (TCC2 is in standby mode). The LEDs should complete this sequence within 5 to 10 minutes.

Step 10 Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue, refer to your next level of support.

Step 11 Repeat Steps 2 through 10 to return the active/standby TCC2 cards to their configuration at the start of the procedure.

Step 12 Verify that the TCC2 cards appear as noted in Step 5.

Step 13 Return to your originating procedure (NTP).

DLP-A255 Cross-Connect Card Side Switch Test

Purpose	This task verifies that the XC, XCVT, and XC10G cards can effectively switch service (active to standby and standby to active).
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Always wait 60 seconds between cross-connect card (side) switches.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the cross-connect cards you are testing to open it in node view.

Step 5 Click the **Maintenance > Cross-Connect** tabs.

Step 6 In the Cross-Connect Cards area, make a note of the active and standby slots.

Step 7 On the shelf graphic, verify that the active cross-connect card has a green ACT LED and the standby cross-connect card has an amber SBY LED. If these conditions are not present, review the "DLP-A37 Install the XC, XCVT, or XC10G Cards" task on page 2-9 or contact your next level of support.

Step 8 Click **Switch**.

Step 9 In the Confirm Switch dialog box, click **Yes**.

Step 10 Verify that the active slot noted in Step 6 becomes the standby slot, and that the standby slot becomes the active slot. The switch should appear within 1 to 2 seconds.

Step 11 Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, do not continue. Refer to your next level of support.

Step 12 Wait 60 seconds, then repeat Steps 7 through 9 to return the active/standby slots to their configuration at the start of the procedure.

Step 13 Verify that the cross-connect card appears as you noted in Step 6.

Step 14 Return to your originating procedure (NTP).

DLP-A88 Optical 1+1 Protection Test

Purpose	This task verifies that a 1+1 protection group will switch traffic properly.
Tools/Equipment	The test set specified by the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24; a test circuit created as part of the topology acceptance test.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 4 On the network map, double-click the node containing the 1+1 protection group you are testing to open it in node view.

Step 5 Click the **Maintenance > Protection** tabs.

Step 6 Initiate a Force switch on the working port:

a. In the Protection Groups area, click the 1+1 protection group.

b. Click the working port. Next to Switch Commands, click **Force**.

c. In the Confirm Force Operation dialog box, click **Yes**.

d. In the Selected Group area, verify that the following appears:

- Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT] [PORT STATE]
- Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 7 Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, complete Step 8, then refer to your next level of support. If a traffic interruption does not occur, complete Steps 8 through 12.

Step 8 Clear the switch on the working port:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

Step 9 Initiate a Force switch on the protect port:

a. In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.

b. In the Confirm Force Operation dialog box, click **Yes**.

c. In the Selected Group area, verify that the following appears:

- Protect port - Protect/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]
- Working port - Working/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 10 Verify that the traffic on the test set connected to the node is still running. If a traffic interruption occurs, complete Step a and then refer to your next level of support. If a traffic interruption does not occur, complete Steps a and 12.

Step 11 Clear the switch on the protect port:

a. Next to Switch Commands, click **Clear**.

b. In the Confirm Clear Operation dialog box, click **Yes**.

c. In the Selected Group area, verify the following states:

- Protect port - Protect/Standby
- Working port - Working/Active

Step 12 Return to your originating procedure (NTP).

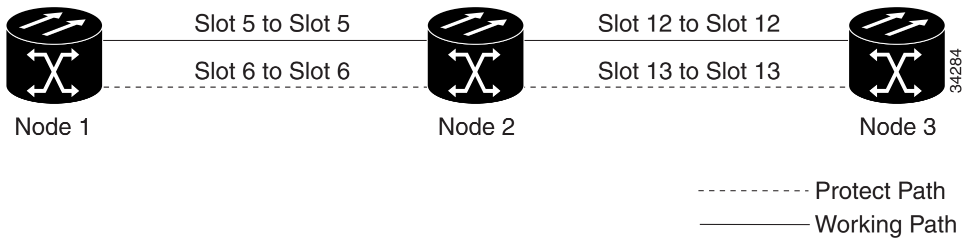
NTP-A38 Provision a Linear ADM Network

Purpose	This procedure provisions three or more ONS 15454s in a linear add-drop multiplexer (ADM) configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at an ONS 15454 where you want to provision in a linear ADM network. If you are already logged in, continue with Step 2.

Figure 6-1 shows three ONS 15454s in a linear ADM configuration. In this example, working traffic flows from Slot 5/Node 1 to Slot 5/Node 2, and from Slot 12/Node 2 to Slot 12/Node 3. Slots 6 and 13 contain the protect OC-N cards. Slots 5 and 6 and Slots 12 and 13 are in 1+1 protection.

Figure 6-1 Linear ADM Configuration



Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards at the node. If the protection group has not been created, complete the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30.

Step 3 Repeat Steps 1 and 2 for all other nodes that you will include in the linear ADM.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, working cards are fibered to working cards and protect cards are fibered to protect cards.

Step 5 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for the working OC-N ports on each linear ADM node.

Note If linear ADM nodes are not connected to a LAN, you will need to create the DCC terminations using a direct (craft) connection to the node. Remote provisioning is possible only after all nodes without LAN connections have DCC terminations provisioned to in-service OC-N ports.

Note Terminating nodes (Nodes 1 and 3 in Figure 6-1) will have one DCC termination, and intermediate nodes (Node 2 in Figure 6-1) will have two DCC terminations (Slots 5 and 12 in the example).

Step 6 Verify that the timing has been set up at each linear node. If not, complete the "NTP-A28 Set Up Timing" procedure on page 4-22. If a node is using line timing, use its working OC-N card as the timing source.

Step 7 Complete the "NTP-A174 Linear ADM Network Acceptance Test" procedure on page 6-13.

Stop. You have completed this procedure.

NTP-A174 Linear ADM Network Acceptance Test

Purpose	This procedure tests a linear ADM network.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on a node in the linear ADM network you are testing. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 5 On the network map, double-click the linear ADM node you are testing to open it in node view.

Step 6 Create a test circuit from that node to an adjacent linear ADM node.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1 card—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS3, then choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 9 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's transmit (Tx) connector; attach the other end to the destination port's receive (Rx) connector.

Step 10 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 11 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 10 to make sure the test set and cabling are configured correctly.

Step 12 Inject BIT errors from the test set. Verify that the errors appear at the test set, indicating a complete end-to-end circuit.

Step 13 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 14 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Step 15 Complete the "DLP-A88 Optical 1+1 Protection Test" task on page 6-11 to test the OC-N port protection group switching.

Step 16 Set up and complete a BER test. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 17 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 18 In network view, click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

Step 19 Delete the test circuit. See the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18.

Step 20 Repeat Steps 6 through 19 for the next linear ADM node you are testing.

Step 21 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

Stop. You have completed this procedure.

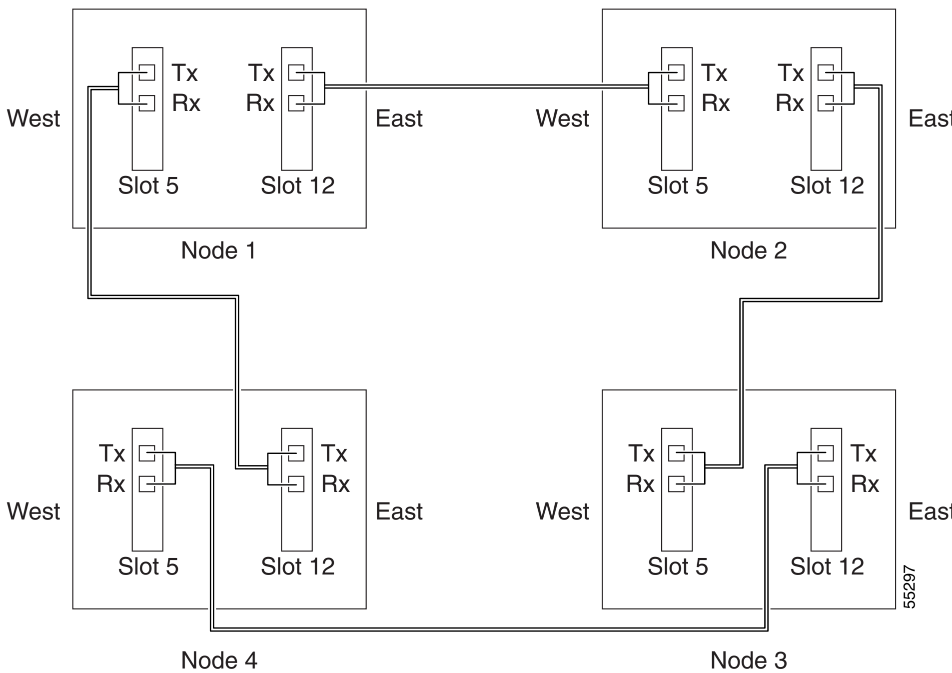
NTP-A40 Provision BLSR Nodes

Purpose	This procedure provisions ONS 15454 nodes for a bidirectional line switched ring (BLSR).
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-37, verifying that the following rules are observed:

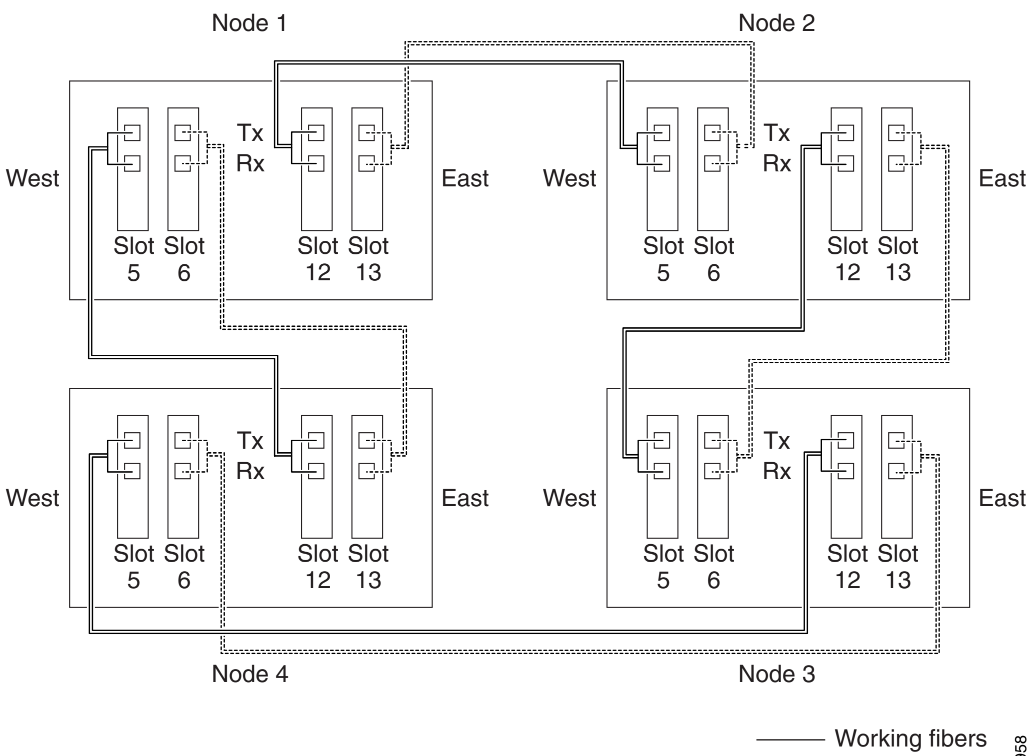
- Verify that the east port at one node is connected to the west port on an adjacent node, and this east to west port connection is used at all BLSR nodes, similar to Figure 6-2. In the figure, the OC-N drop card on the left side of the shelf is the west port, and the drop card on the right side of the shelf is considered the east port.

Figure 6-2 Four-Node, Two-Fiber BLSR Fiber Connection Example



- For four-fiber BLSRs, verify that the same east port to west port connection is used for the working and protect fibers, similar to Figure 6-3. Verify that the working and protect card connections are not mixed. The working cards are the cards where you will provision the DCC terminations.

Figure 6-3 Four-Node, Four-Fiber BLSR Fiber Connection Example



Step 2 Log into an ONS 15454 that you want to configure in a BLSR. See the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4. Provision the two ports/cards that will serve as the BLSR ports at the node. For four-fiber BLSRs, provision the DCC terminations on the OC-N cards that will carry the working traffic, but do not provision DCCs on the protect cards.

Note If an ONS 15454 is not connected to a corporate LAN, DCC provisioning must be performed through a direct (craft) connection to the node. Remote provisioning is possible only after all nodes in the network have DCCs provisioned to in-service OC-N ports.

Step 4 For four-fiber BLSRs, complete the "DLP-A214 Change the Service State for a Port" task on page 6-6 to put the protect OC-N cards/ports in service.

Step 5 If a BLSR span passes through third-party equipment that cannot transparently transport the K3 byte, complete the "DLP-A89 Remap the K3 Byte" task on page 6-18. This task is not necessary for most users.

Step 6 Repeat Steps 2 through 4 at each node that will be in the BLSR. Verify that the EOC (DCC Termination Failure) and LOS (Loss of Signal) are cleared after DCCs are provisioned on all nodes in the ring.

Step 7 Complete the "NTP-A126 Create a BLSR" procedure on page 6-18.

Stop. You have completed this procedure.

DLP-A89 Remap the K3 Byte

Purpose	This task provisions the K3 byte. Do not remap the K3 byte unless specifically required to run an ONS 15454 BLSR through third-party equipment. This task is unnecessary for most users.
Tools/Equipment	OC48AS cards must be installed on the BLSR span that you will remap.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If you remap the K3 byte, remap to the same extended byte (Z2, E2, or F1) on either side of the span.

Step 1 In node view, double-click the OC48AS card that connects to the third-party equipment.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Click **BLSR Ext Byte** and choose the alternate byte: Z2, E2, or F1.

Step 4 Click **Apply**.

Step 5 For four-fiber BLSRs only, repeat Steps 2 through 4 for each protect card.

Step 6 Repeat this task at the node and card on the other end of the BLSR span.

Note The extension byte chosen in Step 3 should match at both ends of the span.

Step 7 Return to your originating procedure (NTP).

NTP-A126 Create a BLSR

Purpose	This procedure creates a BLSR at each BLSR-provisioned node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 6-15
Required/As Needed	As needed; required to complete BLSR provisioning
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you will create the BLSR.

Step 2 Complete one of the following tasks:

- DLP-A328 Create a BLSR Using the BLSR Wizard, page 6-19 – Use this task to create the BLSR using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at once. Using the BLSR wizard is recommended.

- DLP-A329 Create a BLSR Manually, page 6-21 – Use this task to provision the BLSR manually at each node that will be in the BLSR.

Step 3 Complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 6-22 or the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 6-30.

Stop. You have completed this procedure.

DLP-A328 Create a BLSR Using the BLSR Wizard

Purpose	This task creates a BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 6-15
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Create BLSR**.

Step 4 In the BLSR Creation dialog box, set the BLSR properties:

- Ring Type—Choose the BLSR ring type, either two-fiber or four-fiber.
- Speed—Choose the BLSR ring speed: OC-12 (two-fiber BLSR only), OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.

Note If you are creating an OC-12 BLSR and will eventually upgrade it to OC-48 or OC-192, use the single-port OC-12 cards (OC12 IR/STM4 SH 1310, OC12 IR/STM4 SH 1310, or OC12 IR/STM4 SH 1310). You cannot upgrade a BLSR on a four-port OC-12 (OC12/STM4-4) because OC-48 and OC-192 cards are single-port.

- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either upper or lower case letters, this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversions can be set to Never.

For four-fiber BLSRs only, complete the following:

- Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span switch. The default is 5 minutes. Span reversions can be set to Never.

Step 5 Click **Next**. If the network graphic appears, go to Step 6.

If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a "Cannot Create BLSR" message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15, making sure all steps are completed accurately, then start this procedure again.

Step 6 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue and the Finish button appears. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to Step 7 if you are completing a four-fiber BLSR or go to Step 8 if you are completing a two-fiber BLSR.

Step 7 For four-fiber BLSRs, click **Next**. For two-fiber BLSRs go to go to Step 8. In the Protect Port Selection section, choose the protect ports from the West Protect and East Protect columns. Go to the next step.

Step 8 Click **Finish**. If the BLSR window appears with the BLSR you created, go to Step 9. If a "Cannot Create BLSR" or "Error While Creating BLSR" message appears:

a. Click **OK**.

b. In the Create BLSR window, click **Excluded Nodes.** Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms may briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, or BLSROSYNC.

Step 9 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.

Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the "DLP-A326 Change a BLSR Node ID" task on page 15-12.

Step 10 Return to your originating procedure (NTP).

DLP-A329 Create a BLSR Manually

Purpose	This tasks creates a BLSR at each BLSR-provisioned node without using the BLSR wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 6-15 DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Ring** tabs.

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create BLSR dialog box, set the BLSR properties:

- *Ring Type*—Choose the BLSR ring type, either two-fiber or four-fiber.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string "All" in either upper or lower case letters, this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- *Node ID*—Choose a Node ID from the pull-down menu (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
- *Reversion time*—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- *West Line*—Assign the west BLSR port for the node from the pull-down menu.

Note The east and west ports must match the fiber connections and DCC terminations set up in the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15.

- *East Line*—Assign the east BLSR port for the node from the pull-down menu.

For four-fiber BLSRs, complete the following:

- *Span Reversion*—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes. Span reversions can be set to Never. If you set a reversion time, the times must be the same for both ends of the span. That is, if Node A's west fiber is connected to Node B's east port, the Node A west span reversion time must be the same as the Node B east span reversion time. To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.
- *West Protect*—Assign the west BLSR port that will connect to the west protect fiber from the pull-down menu.
- *East Protect*—Assign the east BLSR port that will connect to the east protect fiber from the pull-down menu.

Step 5 Click **OK**.

Note Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6 From the View menu, choose **Go to Other Node**.

Step 7 In the Select Node dialog box, choose the next node that you want to add to the BLSR.

Step 8 Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with Step 9.

Step 9 From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared.

Step 10 Return to your originating procedure (NTP).

NTP-A175 Two-Fiber BLSR Acceptance Test

Purpose	This procedure tests a two-fiber BLSR.
Tools/Equipment	Test set and cables appropriate for the test circuit
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 6-15
	NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform ring switches around the ring. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the East OC-N trunk (span) card of Node 1, "Node 3" refers to the node connected to the East OC-N trunk card of Node 2, and so on.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the ONS 15454s on the BLSR you are testing. (This node will be called Node 1.). If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 5 On the network view, double-click Node 1.

Step 6 Complete the "DLP-A217 BLSR Exercise Ring Test" task on page 6-24.

Step 7 Create a test circuit from Node 1 to the node connected to the east OC-N trunk (span) card of Node 1. (This node will be called Node 2.)

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 8 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS-3, then choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 9 Verify the integrity of all patch cables that will be used in this test by connecting the test set transmit (Tx) connector to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 10 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's transmit (Tx) connector; attach the other end to the port's receive (Rx) connector.

Step 11 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 12 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 1 through 7 to make sure the test set and cabling are configured correctly.

Step 13 Inject BIT errors from the test set. Verify that the errors appear at the test set, verifying a complete end-to-end circuit.

Step 14 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 15 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Although a service interruption under 60 ms may occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 16 Complete the "DLP-A91 BLSR Switch Test" task on page 6-26 at Node 1.

Step 17 Set up and complete a BER test on the test circuit. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 18 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 for the test circuit.

Step 19 Repeating Steps 5 through 18 for Nodes 2 and higher, work your way around the BLSR, testing each node and span in the ring. Create test circuits between every two consecutive nodes.

Step 20 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 21 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 8, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

DLP-A217 BLSR Exercise Ring Test

Purpose	This task tests the BLSR ring functionality without switching traffic. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

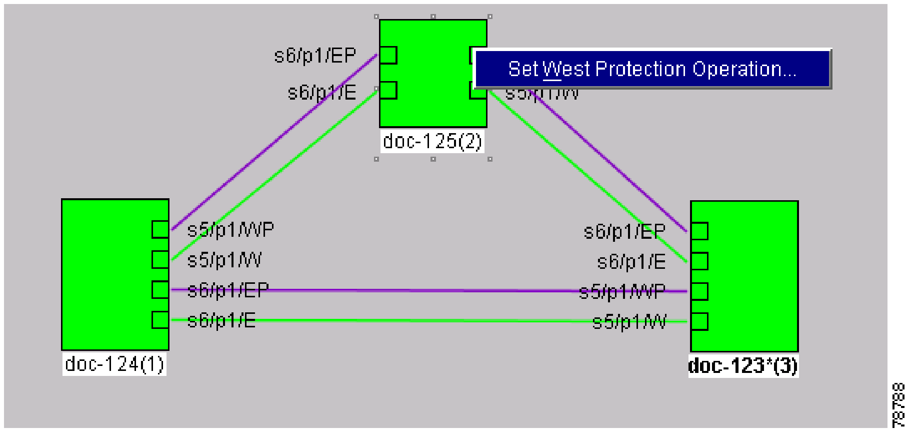
Step 3 Click the row of the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west port:

a. Right-click the west port of any BLSR node and choose **Set West Protection Operation**. Figure 6-4 shows an example. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

> **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. Right-click either working or protect ports.

Figure 6-4 Protection Operation on a Three-Node BLSR



b. In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down menu.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the working BLSR channel where you invoked the protection switch. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Exercise the east port:

a. Right-click the east port of any BLSR node and choose **Set East 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. Right-click either working or protect ports.

b. In the Set East Protection Operation dialog box, choose **EXERCISE RING** from the drop-down menu.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10-15 seconds, then disappear.

Step 6 In the Cisco Transport Controller window, click the **History** tab. Verify that an EXERCISE-RING (Exercising Ring Successfully) condition appears for the node where you exercised the ring. Other conditions that appear include EXERCISE-RING-REQ, KB-PASSTHR, and FE-EXERCISING-RING.

If you do not see any BLSR exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or BLSR drop cards. See the "NTP-A72 Suppress Alarms or Discontinue Alarm Suppression" procedure on page 9-33 for more information.

Step 7 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 8 From the File menu choose **Close** to close the BLSR window.

Step 9 Return to your originating procedure (NTP).

DLP-A91 BLSR Switch Test

Purpose	This task verifies that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the row of the BLSR you will switch, then click **Edit**.

Step 4 Initiate a Force Ring switch the west port:

a. Right-click any BLSR node west port and choose **Set West Protection Operation**. Figure 6-4 on page 6-25 shows an example. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)

> **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. Right-click either working or protect port.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Ring switch. The BLSR span lines turn purple where the switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the West port:

FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.

RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the West line of the node where you performed the switch:

   FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.

   RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.

Step 6 (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, check the following condition. Verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 7 Verify the BLSR line status on each node:

a. From the View menu choose **Go to Node View**.

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

c. Verify the following:

   - The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
   - The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
   - The line states are shown as Act/Act on both East and west sides of the remaining nodes in the ring.

Step 8 From the View menu choose **Go to Network View**.

Step 9 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 10 Display the BLSR window where you invoked the Force Ring switch (the window may be hidden by the CTC window).

Step 11 Clear the switch on the west port:

a. Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set West Protection Operation**.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

   On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines may take a few moments to change color.

Step 12 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 13 Verify the BLSR line status on each node:

a. From the View menu choose **Go to Node View**.

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

b. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 14 Initiate a Force Ring switch on the east port:

a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines are purple where the Force Ring switch was invoked, and all span lines between other BLSR nodes are green. The span lines may take a few moments to change color.

Step 15 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the East port:

- FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

d. Verify that the following conditions are reported on the node that is connected to the East line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.

Step 16 (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 17 Verify the BLSR line status on each node:

a. From the View menu choose **Go to Node View**.

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

c. Verify the following:

- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both East and West sides of the remaining nodes in the ring.

Step 18 From the View menu choose **Go to Network View**.

Step 19 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 20 Display the BLSR window where you invoked the Force Ring switch (the window may be hidden by the CTC window).

Step 21 Clear the switch on the east port:

a. Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines may take a few moments to change color.

Step 22 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 23 Verify the BLSR line status on each node:

a. From the View menu choose **Go to Node View**.

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

c. Verify that the line states are shown as Act/Stby on both the East and west sides of each node in the ring.

Step 24 From the File menu choose **Close** to close the BLSR window.

Step 25 Return to your originating procedure (NTP).

NTP-A176 Four-Fiber BLSR Acceptance Test

Purpose	This procedure tests a four-fiber BLSR.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-A40 Provision BLSR Nodes, page 6-15 NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Note This procedure requires that you create test circuits and perform a ring switch. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the East OC-N trunk (span) card of Node 1, "Node 3" refers to the node connected to the East OC-N trunk card of Node 2, and so on.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on the BLSR you are testing. (This node will be called Node 1.) If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 5 On the network map, double-click Node 1.

Step 6 Complete the "DLP-A92 Four-Fiber BLSR Exercise Span Test" task on page 6-32.

Step 7 Complete the "DLP-A217 BLSR Exercise Ring Test" task on page 6-24.

Step 8 Create a test circuit between Node 1 and Node 2.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS3, then choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end of the cable to the test set transmit (Tx) connector and the other end of the cable to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 11 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's transmit (Tx) connector; attach the other end to the port's receive (Rx) connector.

Step 12 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 13 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 6 through 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject global BIT errors from the test set. Verify that the errors appear at the test set, verifying a complete end-to-end circuit.

Step 15 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 16 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Step 17 Complete the "DLP-A91 BLSR Switch Test" task on page 6-26 to test the BLSR protection switching at Node 1.

Step 18 Complete the "DLP-A93 Four-Fiber BLSR Span Switching Test" task on page 6-34 at Node 1.

Step 19 Set up and complete a BER test on the test circuit between Node 1 and 2. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 20 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 for the test circuit.

Step 21 At Node 2, repeat Steps 5 through 20, creating a test circuit between Node 2 and the node connected to the east OC-N trunk (span) card of Node 2 (Node 3). Work your way around the BLSR creating test circuits between every two consecutive nodes.

Step 22 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 23 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 24 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 25 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 8, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

DLP-A92 Four-Fiber BLSR Exercise Span Test

Purpose	This task exercises a four-fiber BLSR span. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west span:

a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

Note The squares on the network map represent ports. Right-click a working port.

b. In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down menu.

c. Click **OK**. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10-15 seconds, then disappear.

Step 5 Verify the conditions:

a. Click the **Conditions** tab, then click **Retrieve**.

b. Verify the following conditions:

- EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
- FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the East span of the node connected to the west side of the node where you exercised the span.
- KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Exercise the east span:

a. Right-click the east port of the four-fiber BLSR node that you want to exercise and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down menu.

c. Click **OK**.

d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 8 From the File menu, choose **Close**.

Step 9 Verify the conditions:

a. Click the **Conditions** tab, then click **Retrieve**.

b. Verify the following conditions:

- EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
- FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the East span of the node connected to the west side of the node where you exercised the span.
- KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 10 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 11 From the File menu choose **Close** to close the BLSR window.

Step 12 Return to your originating procedure (NTP).

DLP-A93 Four-Fiber BLSR Span Switching Test

Purpose	This task verifies that traffic will switch from working to protect fibers on a four-fiber BLSR span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**. A BLSR window appears containing a graphic of the BLSR.

> **Note** If the node icons are stacked on the BLSR graphic, press Ctrl while you drag and drop each one to a new location so you can see the BLSR port information clearly.

Step 4 Switch the west span:

a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. Figure 6-4 on page 6-25 shows an example.

> **Note** The squares on the network map represent ports. Right-click a working port.

b. In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the Force Span switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that a SPAN-SW-WEST (Span Switch West) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-EAST (Span Switch East) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Display the BLSR window where you invoked the Force Span switch (the window may be hidden by the CTC window).

Step 8 Clear the west switch:

a. Right-click the west port of the BLSR node where you invoked the Force Span switch and choose **Set West Protection Operation**.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F disappears, and the span lines between BLSR nodes will be purple and green. The span lines may take a few moments to change color.

Step 9 Switch the east span:

a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **FORCE SPAN** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Span switch. The BLSR span lines are purple where the Force Span switch was invoked, and all span lines between other BLSR nodes are green. The span lines may take a few moments to change color.

Step 10 Verify the conditions:

a. Click the **Conditions** tab.

b. Click **Retrieve**.

c. Verify that a SPAN-SW-EAST (Span Switch East) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-WEST (Span Switch West) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off.

Step 11 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 12 Display the BLSR window where you invoked the Force Span switch (the window may be hidden by the CTC window).

Step 13 Clear the east switch:

a. Right-click the east port of the BLSR node where you invoked the Force Span switch and choose **Set East Protection Operation**.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu.

c. Click **OK**.

d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines may take a few moments to change color.

Step 14 From the File menu, choose **Close** to close the BLSR window.

Step 15 Return to your originating procedure (NTP).

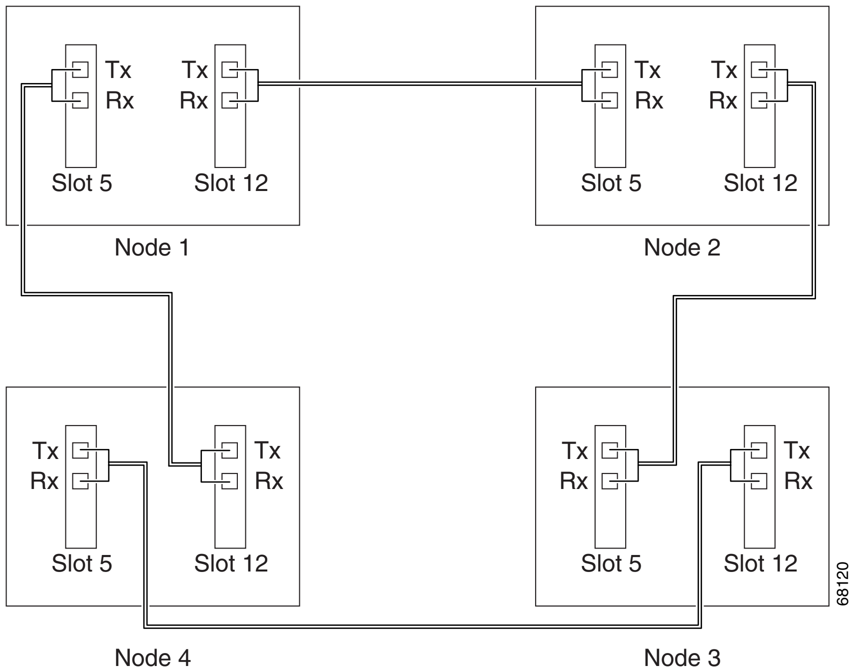
NTP-A44 Provision Path Protection Nodes

Purpose	This procedure provisions nodes for inclusion in a path protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The path protection is the default ONS 15454 topology. It is available as soon as you install the path protection OC-N cards, connect the OC-N fibers, and create the DCC terminations. Unlike the BLSRs, ONS 15454 path protection configurations do not require explicit set up.

Step 1 Verify that the fiber is correctly connected to the path protection trunk (span) OC-N cards similar to Figure 6-5. See the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Figure 6-5 Path Protection Fiber Connection Example



Step 2 Log into an ONS 15454 in the path protection you are turning up. See the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 or "DLP-A355 Provision SONET LDCC Terminations" task on page 6-5 for the two cards/ports that will serve as the path protection ports on the node, for example, Slot 5 (OC-48)/Node 1 and Slot 12 (OC-48)/Node 1.

> **Note** If an ONS 15454 is not connected to a corporate LAN, DCC or LDCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have DCC or LDCC terminations provisioned to in-service OC-N ports.

Step 4 Repeat Steps 2 and 3 for each node in the path protection.

Step 5 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38.

Stop. You have completed this procedure.

NTP-A177 Path Protection Acceptance Test

Purpose	This procedure tests a path protection.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 6-36
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the ONS 15454s on the path protection you are testing. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from that node to the next adjacent path protection node.

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS3, then choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 8 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 9 Create a physical loopback at the circuit destination card:

a. Attach one end of a patch cable to the destination port's transmit (Tx) connector.

b. Attach the other end to the port's receive (Rx) connector.

Step 10 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 11 Verify that the test set has a clean signal. If a clean signal does not appear, repeat Steps 1 through 8 to make sure the test set and cabling are configured correctly.

Step 12 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors appear at the test set.

Step 13 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 14 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Step 15 From the View menu, choose **Go to Network View**.

Step 16 Click one of the two spans leaving the circuit source node.

Step 17 Complete the "DLP-A94 Path Protection Switching Test" task on page 6-40 to test the path protection protection switching function on this span.

Step 18 In network view, click the other circuit source span and repeat Step 17.

Step 19 Set up and complete a BER Test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 20 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 for the test circuit.

Step 21 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 22 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 23 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 24 Repeat Steps 6 through 20 for each node on the network.

Step 25 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 8, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

DLP-A94 Path Protection Switching Test

Purpose	This task verifies that a path protection span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Although a service interruption under 60 ms may occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 1 From the View menu, choose **Go to the Network View**.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

a. Click the **Perform UPSR span switching** field.

b. Choose **FORCE SWITCH AWAY** from the drop-down menu.

c. Click **Apply**.

d. In the Confirm UPSR Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the Switch State for all circuits is FORCE. Unprotected circuits will not switch.

Step 4 Clear the Force switch:

a. Click the **Perform UPSR span switching** field and choose **CLEAR** from the drop-down menu.

b. Click **Apply**.

c. In the Confirm UPSR Switch dialog box, click **Yes**.

d. 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.

Step 5 Return to your originating procedure (NTP).

NTP-A216 Provision a Traditional Path Protection Dual Ring Interconnect

Purpose	This procedure provisions path protection configurations in a traditional dual ring interconnect (DRI) topology. DRIs interconnect two or more path protection configurations to provide an additional level of protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note To route circuits on the DRI, you must check the Dual Ring Interconnect check box during circuit creation.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, go to Step 3.

a. Complete the "NTP-A44 Provision Path Protection Nodes" procedure on page 6-36 to provision the path protection configurations.

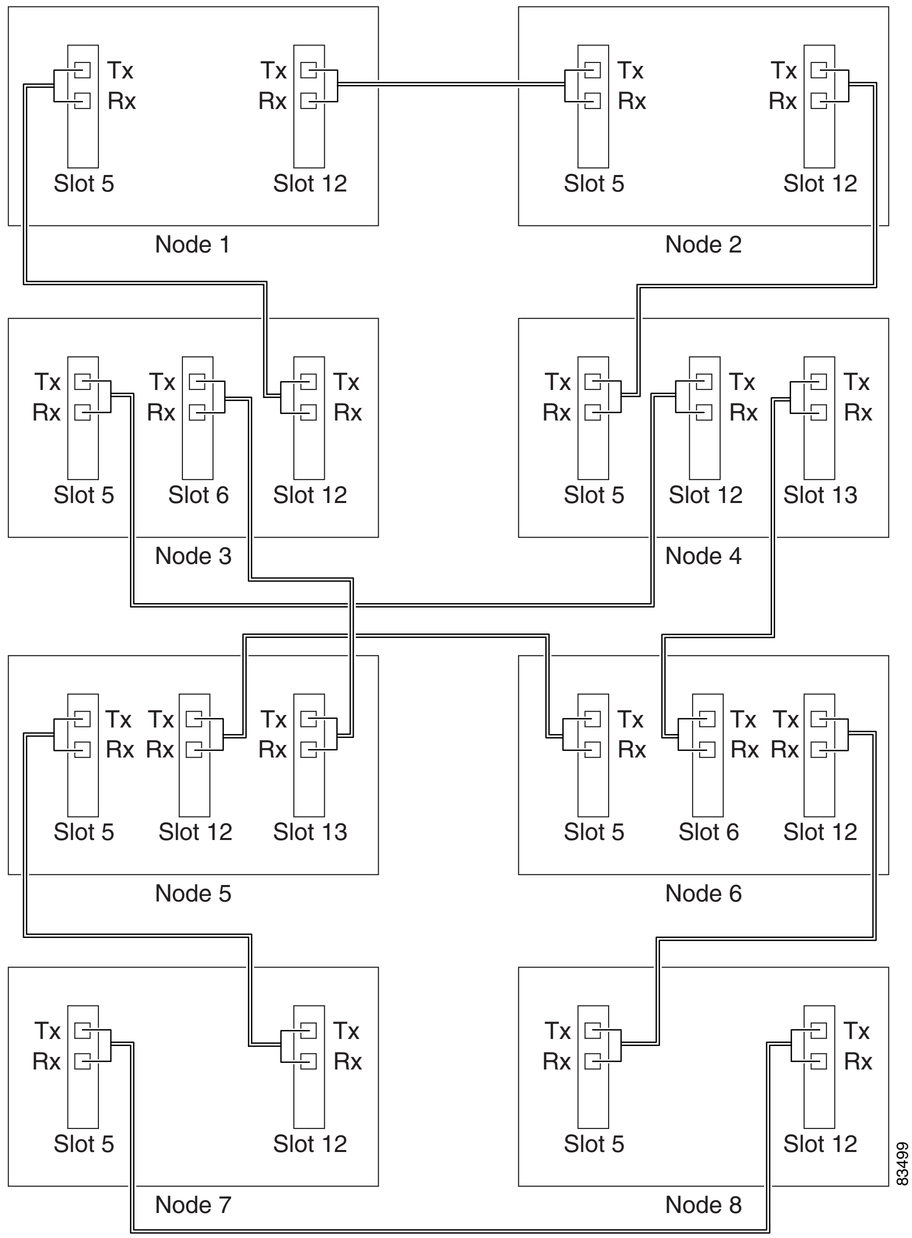
b. Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38 to test the path protection configurations.

Note All path protection configurations that will be interconnected must have the same OC-N rate.

Step 3 Verify that the path protection DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the path protection configurations must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have fiber connections. An example is shown in Figure 6-6. This example shows a path protection DRI with two rings, Nodes 1 through 4 and 5 through 8. In the example, an additional OC-N is installed in Slot 13 at Node 4 and connected to an OC-N in Slot 6 at Node 6. Nodes 3 and 5 are interconnected with OC-N cards in Slot 6 (Node 3) and Slot 13 (Node 5).

Figure 6-6 Traditional Path Protection DRI Fiber Connection Example



Stop. You have completed this procedure.

NTP-A217 Provision an Integrated Path Protection Dual Ring Interconnect

Purpose	This procedure provisions path protection configurations in an integrated dual ring interconnect (DRI) topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node in the path protection DRI network. If you are already logged in, continue with Step 2.

Step 2 Complete the following steps if you have not provisioned the path protection configurations that you will interconnect in a path protection DRI. If the path protection configurations are created, continue with Step 3.

a. Complete the "NTP-A44 Provision Path Protection Nodes" procedure on page 6-36 to provision the path protection configurations.

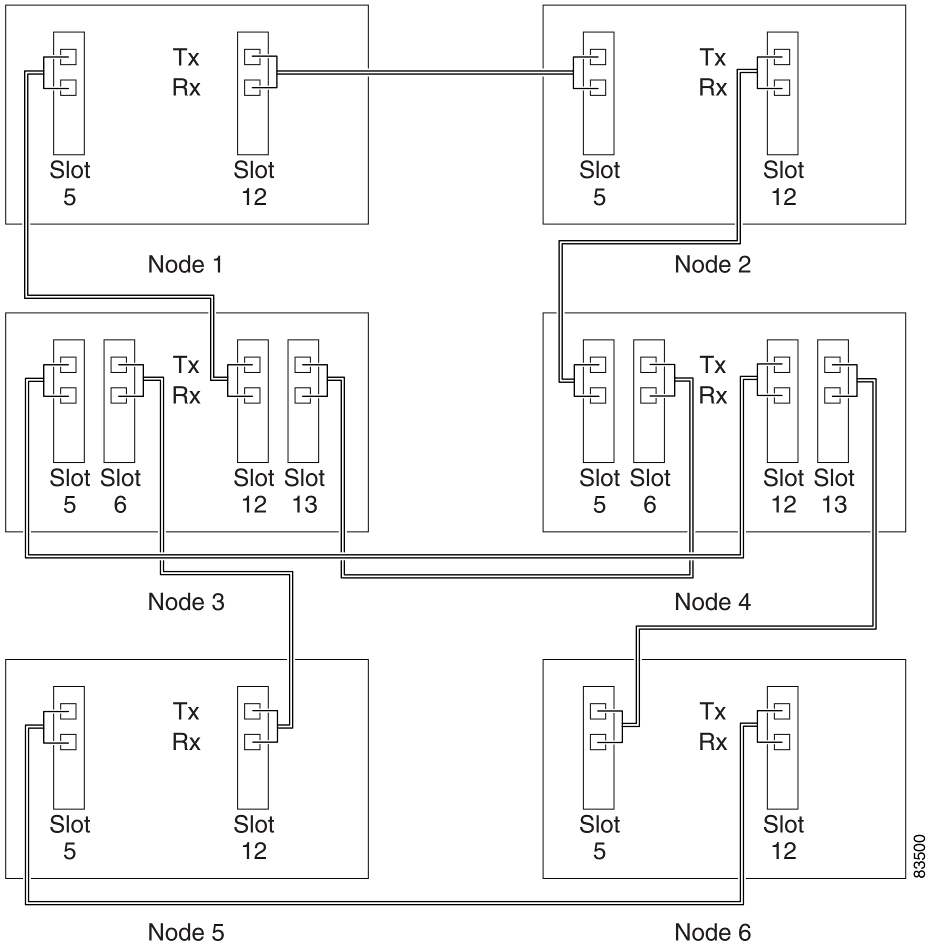
b. Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38 to test the path protection configurations.

Note All path protection configurations that will be interconnected must have the same OC-N rate.

Step 3 Verify that the path protection DRI interconnect nodes have OC-N cards installed and have fiber connections to the other interconnect node:

- The OC-N cards that will connect the path protection configurations must be installed at the interconnect nodes. The OC-N cards in the path protection nodes and the interconnect nodes must be the same type.
- The interconnect nodes must have the correct fiber connections. An example is shown in Figure 6-7. This example shows a path protection DRI with two rings.

Figure 6-7 Integrated Path Protection DRI Example



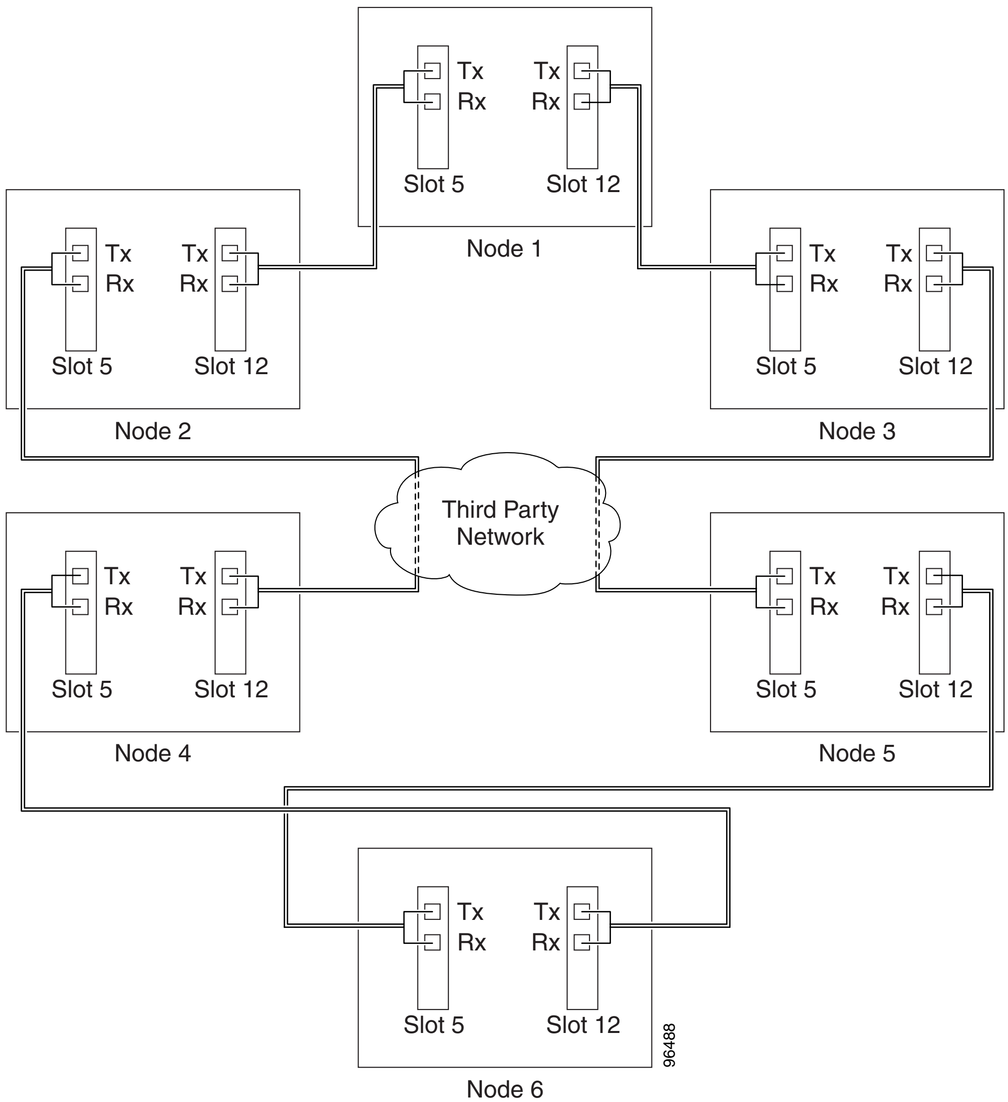
Stop. You have completed this procedure.

NTP-A224 Provision an Open-Ended Path Protection

Purpose	This procedure provisions ONS 15454s in an open-ended path protection configurations connected to a third-party vendor network. This topology allows you to route a circuit from one ONS 15454 network to another ONS 15454 network through the third-party network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the path protection trunk (span) OC-N cards at each open-ended path protection node. Figure 6-8 shows an example. Node 1 is connected to ONS 15454 Nodes 2 and 3 through Slots 12 and 5. Trunk cards at Nodes 2 and 3 are connected to the third-party vendor equipment.

Figure 6-8 ONS 15454 Open-Ended Path Protection Fiber Connection Example



Step 2 Verify that the third-party cards or units to which the ONS 15454 trunk cards are connected are the same OC-N rate as the ONS 15454 trunk cards. The third-party time slots must match the ONS 15454 card time slots to which they are connected. For example, if your trunk card is an OC-48, the third-party vendor card or unit must have STSs 1-48 available.

Step 3 Log into an ONS 15454 in the path protection you are turning up. See the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 4.

Step 4 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 or "DLP-A355 Provision SONET LDCC Terminations" task on page 6-5 for the ONS 15454 cards/ports that are connected to another ONS 15454. Do not create DCC or LDCC terminations for the card/port that connects to the third-party equipment. For example in Figure 6-8, DCC terminations are created at the following cards/ports:

- Nodes 1 and 6: Slot 5 and Slot 12
- Node 2 and 5: Slot 12
- Node 3 and 4: Slot 5

Note If an ONS 15454 is not connected to a corporate LAN, DCC or LDCC provisioning must be performed through a direct (craft) connection. Remote provisioning is possible only after all nodes in the network have DCC or LDCC terminations provisioned to in-service OC-N ports.

Step 5 Repeat Steps 3 through 4 for each node in the path protection.

Step 6 Following the documentation provided by the third-party vendor, provision the optical loop leading from the ONS 15454 connection at one end to the ONS 15454 connection at the other end. In other words, you will create an open-ended path protection using procedures for the third-party equipment.

Step 7 Complete the "NTP-A225 Open-Ended Path Protection Acceptance Test" procedure on page 6-46.

Stop. You have completed this procedure.

NTP-A225 Open-Ended Path Protection Acceptance Test

Purpose	This procedure tests an open-ended path protection.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create.
Prerequisite Procedures	NTP-A224 Provision an Open-Ended Path Protection, page 6-44
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure might be service affecting if performed on a node carrying traffic.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that will be the source node for traffic traversing the third-party network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 4 Click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 5 On the network map, double-click the node that you logged into in Step 1.

Step 6 Create a test circuit from that node to the OC-N trunk (span) cards on the nodes that connect to the third-party network. For example, in Figure 6-8 on page 6-45, a circuit is created from Node 1 to the Slot 5 OC-N card at Node 2, and a secondary circuit destination is created on the Slot 12 OC-N card at Node 3. For circuit creation procedures, complete one of the following:

- For DS-1 circuits, complete the "NTP-A181 Create an Automatically Routed DS-1 Circuit" procedure on page 8-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-A184 Create an Automatically Routed DS-3 Circuit" procedure on page 8-22. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For OC-N circuits, complete the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 7 Create a circuit within the third-party network from ONS 15454 connection ports to the second set of ONS 15454 connection ports on both path protection spans. Refer to the third-party equipment documentation for circuit creation procedures.

Step 8 Repeat Step 6 to create a second circuit at the terminating node on the other side of the third-party network. In Figure 6-8, this is Node 6. However, this circuit will have two sources, one at Node 4/Slot 12, and one at Node 5/Slot 5. The destination will be a drop card on Node 6.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a muxed DS3, then choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.
- OC-N—If you are testing an OC-N circuit, set the test set for the applicable circuit size. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 11 Create a physical loopback at the circuit destination card:

a. Attach one end of a patch cable to the destination port's transmit (Tx) connector.

b. Attach the other end to the port's receive (Rx) connector.

Step 12 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 13 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 1 through 8 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors appear at the test set.

Step 15 Complete the "DLP-A356 TCC2 Active/Standby Switch Test" task on page 6-9.

Step 16 Complete the "DLP-A255 Cross-Connect Card Side Switch Test" task on page 6-10.

Although a service interruption under 60 ms may occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 17 From the View menu, choose **Go to Network View**.

Step 18 Click one of the two spans leaving the circuit source node.

Step 19 Complete the "DLP-A94 Path Protection Switching Test" task on page 6-40 to test the path protection switching function on this span.

Step 20 In network view, click the other circuit source span and repeat Step 19.

Step 21 Set up and complete a BER Test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 22 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 for the test circuit.

Step 23 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 24 In network view, click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

c. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the alarm information.

Step 25 In network view, click the **Conditions** tab.

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide if necessary.*

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export the conditions information.

Step 26 Repeat Steps 6 through 25 for each node that will be a source or destination for circuits traversing the third-party network.

Step 27 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 8, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

NTP-A46 Subtend a Path Protection from a BLSR

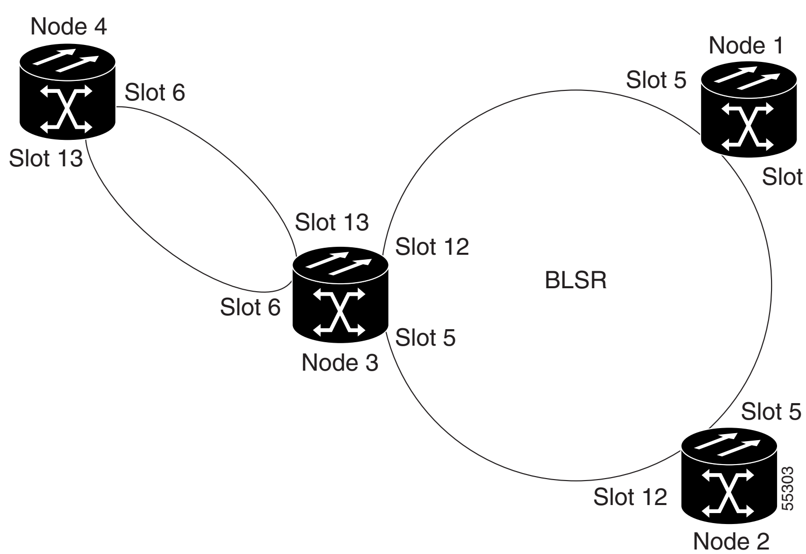
Purpose	This procedure subtends a path protection from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers to carry the path protection.
Prerequisite Procedures	NTP-A175 Two-Fiber BLSR Acceptance Test, page 6-22 or NTP-A176 Four-Fiber BLSR Acceptance Test, page 6-30
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note The path protection is the default ONS 15454 topology. It is available as soon as you install the path protection OC-N cards, connect the OC-N fibers, and create the DCC terminations. Unlike the BLSRs, ONS 15454 path protection configurations do not require explicit set up.

Step 1 In the node that will subtend the path protection (Node 3 in Figure 6-9), install the two OC-N cards that will serve as the path protection trunk (span) cards (Node 3, Slots 6 and 13). See the "NTP-A16 Install the OC-N Cards" procedure on page 2-12. If they are already installed, continue with Step 2.

Step 2 Attach fibers from these cards to the path protection trunk cards on the neighbor path protection node or nodes. In Figure 6-9, Node 3/Slot 6 connects to Node 4/Slot 13, and Node 3/Slot 13 connects to Node 4/Slot 6.

Figure 6-9 Path Protection Subtended from a BLSR



Step 3 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the ONS 15454 that will subtend the path protection (Node 3 in the example).

Step 4 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for each OC-N card that will carry the path protection.

Step 5 Log into a path protection node that connects to the node in Step 3. (In Figure 6-9, Node 4 is the only other node in the path protection.)

Step 6 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for each OC-N card that will carry the path protection.

Step 7 Repeat Step 6 for each node in the path protection.

Step 8 From the View menu, choose **Go To Network View** to view the subtending rings.

Step 9 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38.

Stop. You have completed this procedure.

NTP-A47 Subtend a BLSR from a Path Protection

Purpose	This procedure subtends a BLSR from an existing path protection.
Tools/Equipment	One path protection node must have OC-N cards and fibers to carry the BLSR
Prerequisite Procedures	NTP-A177 Path Protection Acceptance Test, page 6-38
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the path protection node that will subtend the BLSR, install the two OC-N cards that will serve as the BLSR trunk (span) cards (in Figure 6-9 on page 6-49, Node 3, Slots 5 and 12). See the "NTP-A16 Install the OC-N Cards" procedure on page 2-12.

Step 2 Attach fibers from the cards in Step 1 to the BLSR trunk cards on another BLSR node or nodes. In Figure 6-9, Slot 5/Node 3 connects to Slot 12/Node 2, and Slot 12/Node 3 connects to Slot 5/Node 1.

Step 3 Log into the ONS 15454 that will subtend the BLSR (the node in Step 1). See the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 4.

Step 4 Create the DCCs on both OC-N trunk cards (east and west) that will carry the BLSR. See the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4.

Step 5 Create the subtending BLSR:

a. Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

b. Complete the "NTP-A126 Create a BLSR" procedure on page 6-18. Include the node in Step 3 (the node that will subtend the BLSR) in the BLSR.

Step 6 From the View menu, choose **Go to the Network View** to see the subtending ring.

Stop. You have completed this procedure.

NTP-A48 Subtend a BLSR from a BLSR

Purpose	This procedure subtends a BLSR from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers needed to carry the second BLSR.
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

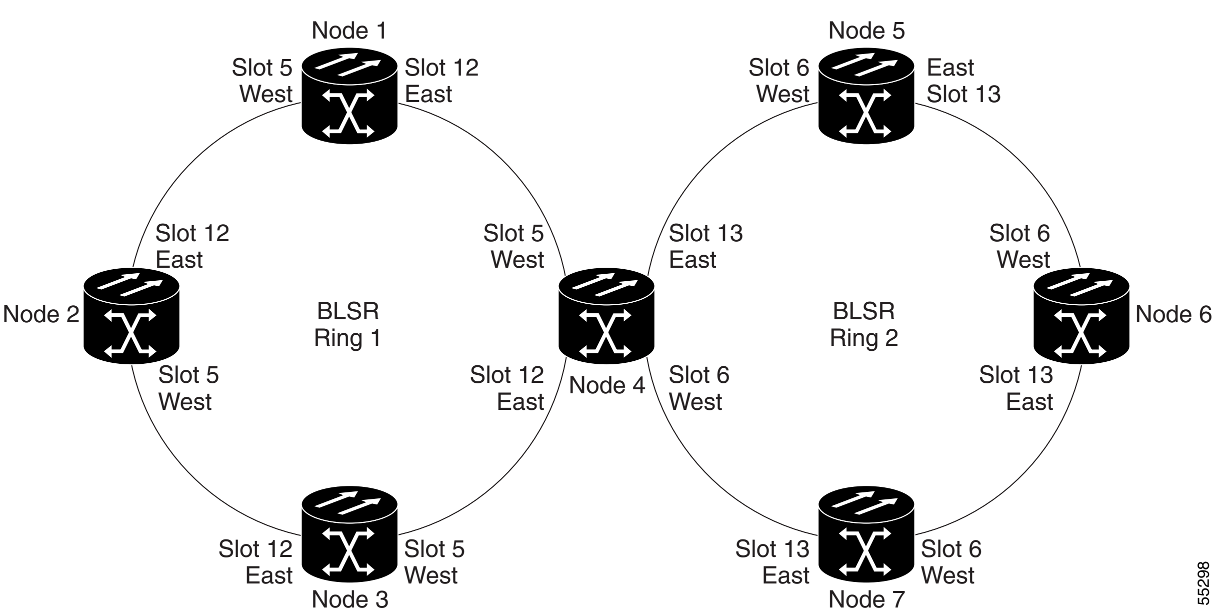
Note This procedure assumes that all nodes are configured for the BLSR. If you need to add a node to a BLSR, see the "NTP-A212 Add a BLSR Node" procedure on page 16-1.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that will subtend the BLSR (Node 4 in Figure 6-10). If you are already logged in, continue with Step 2.

Step 2 Install the OC-N cards that will serve as the BLSR trunk (span) cards if they are not already installed. See the "NTP-A16 Install the OC-N Cards" procedure on page 2-12.

Figure 6-10 shows two BLSRs shared by one ONS 15454. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7 and represents the subtending ring added by this procedure. Two BLSR rings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 5 and 12, and Ring 2 uses cards in Slots 6 and 13.

Figure 6-10 BLSR Subtended from a BLSR



Step 3 Attach fibers from the trunk cards in the subtending node to the BLSR trunk cards on its two neighboring BLSR nodes. In Figure 6-10, Node 4/Slot 6 connects to Node 7/Slot 13, and Node 4/Slot 13 connects to Node 5/Slot 6.

Step 4 Create the DCCs on the first OC-N card that will carry the BLSR. See the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4.

Step 5 Repeat Step 4 for the second OC-N trunk card that will carry the BLSR.

Step 6 Complete the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

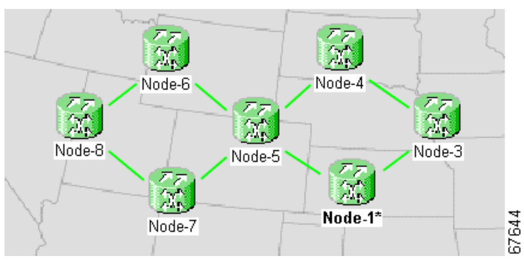
Step 7 If the subtending BLSR is not already created, complete the "NTP-A126 Create a BLSR" procedure on page 6-18 to provision the new BLSR. The subtending BLSR must have a ring name that differs from the ring name of the first BLSR.

> **Note** The subtending node can have one Node ID that is used in both BLSRs, or a different Node ID for each BLSR. For example, the same node can be Node 4 in BLSR 1 and Node 2 in BLSR 2.

Step 8 From the View menu, choose **Go to Network View** to see the subtending ring.

Figure 6-11 shows an example of two subtending BLSRs.

Figure 6-11 Subtended BLSRs on the Network Map



Stop. You have completed this procedure.

NTP-A172 Create a Logical Network Map

Purpose	This procedure positions nodes in the network view and allows a Superuser to create a consistent network view for all nodes on the network.
Tools	None
Prerequisite Procedures	This procedure assumes that network turn up is complete.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on an ONS 15454 on the network where you want to create the network map. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Change the position of the nodes in the network view according to your site plan.

a. Click a node to select it, then press the **Ctrl** key while you drag and drop a node icon to a new location.

b. Deselect the previously selected node by clicking on any blank part of the network map area.

c. Repeat Step a for each node you need to position.

Step 4 On the network view map, right-click and choose **Save Node Position**.

Step 5 Click **Yes** in the Save Node Position dialog box.

CTC displays a progress bar and saves the new node positions.

Note Retrieve, Provisioning, and Maintenance users can move nodes on the network map, but only Superusers can save new network map configurations. To restore the view to a previously saved version of the network map, right-click on the network view map and choose Reset Node Position.

Stop. You have completed this procedure.

CHAPTER 7

Turn Up DWDM Network

This chapter explains how to turn up and test a Cisco ONS 15454 dense wave division multiplexing (DWDM) network. For DWDM topology reference information and span loss tables, refer to the "DWDM Topologies" chapter in the *Cisco ONS 15454 Reference Manual*.

There are two main DWDM network types, metro core, where the channel power is equalized and dispersion compensation is applied, and metro access, where the channels are not equalized and dispersion compensation is not applied. Metro Core networks often include multiple spans and amplifiers, thus making optical signal to noise ratio (OSNR) the limiting factor for channel performance. Metro Access networks often include a few spans with very low span loss; therefore, the signal link budget is the limiting factor for performance. The DWDM network topologies supported are hubbed rings, multihubbed rings, meshed rings, linear configurations, and single-span links.

The DWDM node types supported are hub, terminal, optical add/drop multiplexing (OADM), anti-amplified spontaneous emissions (ASE), and line amplifier. The hybrid node types supported are 1+1 protected flexible terminal, scalable terminal, hybrid terminal, hybrid OADM, hybrid line amplifier, and amplified time division multiplexing (TDM). For DWDM and hybrid node turn up procedures, see Chapter 5, "Turn Up a DWDM Node."

Note To support pure DWDM or hybrid networks, the ONS 15454 must be running Software Release 4.6.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A232 Verify DWDM Node Turn Up, page 7-2—Complete this procedure before beginning network turn up.
2. NTP-A280 Provision DWDM or Hybrid Network Connections, page 7-3—Complete this procedure to provision OSC, GCC, LDCC or DCC connections and to check span attenuation as needed.
3. NTP-A281 Provision and Verify a DWDM Network, page 7-11—Complete as needed.
4. NTP-A282 Verify the Optical Receive Power, page 7-18—Complete as needed.
5. NTP-A283 Verify the OSNR, page 7-19—Complete as needed.
6. NTP-A284 Convert a Pass-Through Connection to an Add/Drop Connection, page 7-20—Complete as needed.

NTP-A232 Verify DWDM Node Turn Up

Purpose	This procedure verifies that each ONS 15454 is ready for DWDM network turn up before adding nodes to a network.
Tools/Equipment	None
Prerequisite Procedures	Chapter 5, "Turn Up a DWDM Node"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the network that you will test. See the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, proceed to Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the alarm filter is not turned on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 3 Verify that the software version and Defaults shown in the node view status area match the software version and NE defaults shown in your site plan. If either are not correct, complete the following procedures as needed:

- If the software is not the correct version, install the correct version from the ONS 15454 software CD. Upgrade procedures are located in the *Cisco ONS 15454 Software Upgrade Guide*. Follow the upgrade procedures appropriate to the software currently installed on the node. TCC2 cards can also be ordered with the latest software release.
- If the node defaults are not correct, import the network element defaults. Refer to the *Cisco ONS 15454 Network Element Defaults* for Software R4.6.

Step 4 Click the **Provisioning > General** tabs. Verify that all general node information settings match the settings of your site plan. If not, see the "NTP-A81 Change Node Management Information" procedure on page 12-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that timing settings match the settings of your site plan. If not, see the "NTP-A85 Change Node Timing" procedure on page 12-23.

Step 6 Click the **Provisioning > Network** tabs. Ensure that the IP settings and other Cisco Transport Controller (CTC) network access information is correct. If not, see the "NTP-A201 Change CTC Network Access" procedure on page 12-4.

Step 7 Click the **Provisioning > Protection** tabs. Verify that all protection groups have been created according to your site plan. If not, see the "NTP-A203 Modify or Delete Card Protection Settings" procedure on page 12-15.

Step 8 Click the **Provisioning > Security** tabs. Verify that all users have been created and that their security levels match the settings indicated by your site plan. If not, see the "NTP-A205 Modify Users and Change Security" procedure on page 12-25.

Step 9 If Simple Network Management Protocol (SNMP) is provisioned on the node, click the **Provisioning > SNMP** tabs. Verify that all SNMP settings match the settings of your site plan. If not, see the "NTP-A87 Change SNMP Settings" procedure on page 12-33.

Step 10 Provision the network connections using the "NTP-A280 Provision DWDM or Hybrid Network Connections" procedure on page 7-3.

Stop. You have completed this procedure.

NTP-A280 Provision DWDM or Hybrid Network Connections

Purpose	This procedure verifies OSC terminations, provisions GCC terminations, and checks span attenuation. Cross-references are also provided for LDCC and DCC terminations if they are required for your hybrid network. For more information about DWDM and hybrid topologies, refer to the "DWDM Topologies" chapter in the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	None
Prerequisite Procedures	NTP-A232 Verify DWDM Node Turn Up, page 7-2
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Check the fiber connections. See the "NTP-A244 Install Fiber-Optic Cables on DWDM Cards" procedure on page 2-41 for instructions.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24.

Step 3 Verify the OSC terminations from the **Provisioning > DCC/GCC/OSC > OSC** tabs. All termination alarms disappear after the terminations are created for each node in your site plan and the correct port is in the IS state. If the OSC terminations were created correctly, complete Step 5. If problems occurred with the OSC terminations, complete Steps 4 and 5.

Step 4 If the OSC link is not working or the span measurement is not consistent with the value shown in the MetroPlanner file, Cisco qualified personnel must measure the span insertion loss by using an optical time domain reflectometer (OTDR).

Note For information about using an OTDR, refer to the OTDR user guide.

OTDR measurement requires the far-end fiber to be disconnected. If the new span insertion loss value is acceptable, a new MetroPlanner configuration file is generated.

Step 5 Complete the "DLP-A344 Check OSC Span Attenuation" task on page 7-5.

Step 6 If you are setting up a hybrid DWDM network, complete the following, as necessary, after you have checked span attenuation:

a. Provision any of the following:

- DLP-A354 Provision SONET DCC Terminations, page 6-4
- DLP-A355 Provision SONET LDCC Terminations, page 6-5
- DLP-A343 Provision GCC Terminations, page 7-4

Note Perform this procedure before you create circuits for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards.

b. Verify the GCC, DCC, or LDCC terminations. All termination alarms disappear after the terminations are created for each node in your site plan and the correct port is in the IS state. If problems occurred with the GCC, DCC, or LDCC terminations, repeat Step 6 and make sure terminations were created for all nodes in your site.

Step 7 Complete the "DLP-A345 Provision the Ring ID" task on page 7-9.

Stop. You have completed this procedure.

DLP-A343 Provision GCC Terminations

Purpose	This task creates the DWDM GCC terminations required for network setup when using the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards. Perform this task before you create circuits for these cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view click the **Provisioning > DCC/GCC/OSC > GCC** tabs.

Step 2 In the GCC Terminations pane, click **Create.**

Step 3 In the Create optical transport network (OTN) GCC Terminations dialog box, click the ports where you want to create the GCC termination. To select more than one port, press the **Shift** key or the **Ctrl** key.

Note GCC refers to the G.709 communications channel, which is used for ONS 15454 transponders and muxponders in DWDM applications.

Step 4 (Optional) From the GCC Rate drop-down menu, choose from two options:

- 192k is the line rate of Section DCC (SDCC)—This is the default option in Software R4.6.
- 576k is the line rate of Line DCC (LDCC)—This option will be supported in a future software release.

Step 5 Click **Set to IS** if you want to put ports in service.

Step 6 Click **OK**. Until all network GCC terminations are created and the ports are in service, GCC-EOC alarms appear.

Step 7 Return to your originating procedure (NTP).

DLP-A344 Check OSC Span Attenuation

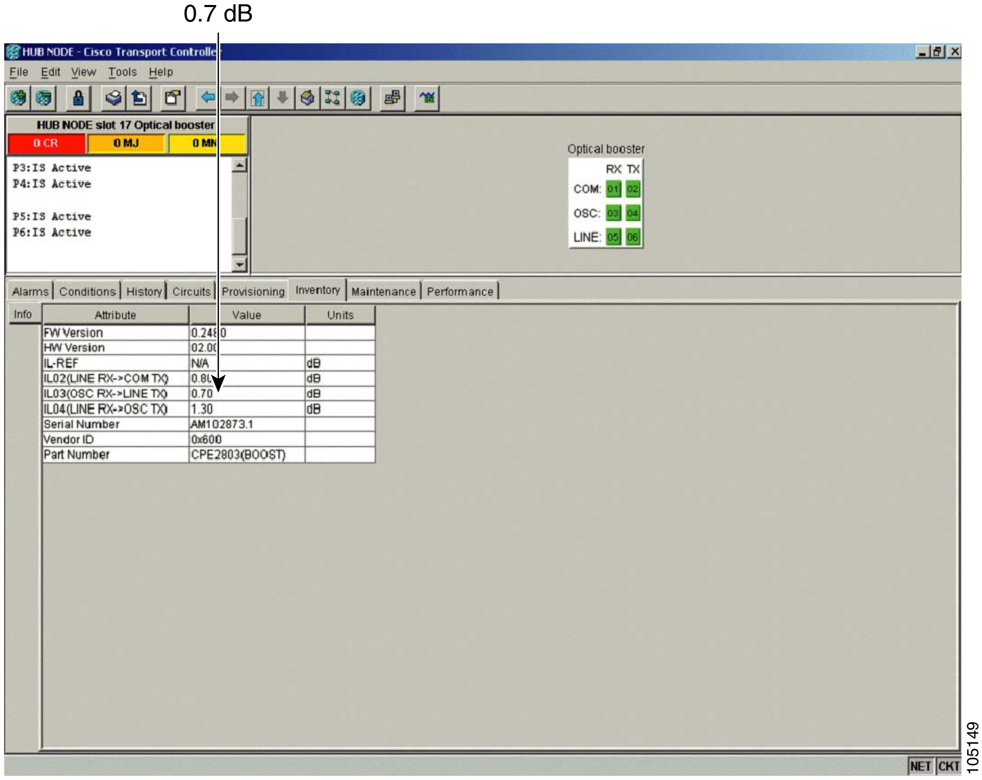
Purpose	This task checks OSC span attenuation between two DWDM nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Check span attenuation by calculating the difference between transmitted OSC power at the beginning of the span and the received OSC power at the end of the span. These calculated values must be consistent with the data provided by the MetroPlanner installation file, plus or minus 2 dB. The MetroPlanner span losses are read directly from the network diagram.

- To read the transmit power on an OSCM card at the beginning of the span, double-click the OSCM card in node view and click the **Provisioning > Optical Line > Parameters** tabs. Make note of the line-Tx (OSC output) power level listed in the Power field for the row labeled as 3 LINE-X-1-TX where X equals 8 or 11. Next go to the associated downstream OPT-BST card view and click the **Inventory** tab (Figure 7-1). Find the row labeled IL03(OSC RX->LINE TX). Make note of this insertion loss listed in the Value field. Subtract this OPT-BST insertion loss from the OSCM TX power level. Use this value and subtract it from the power level on the receiver to calculate the span loss.

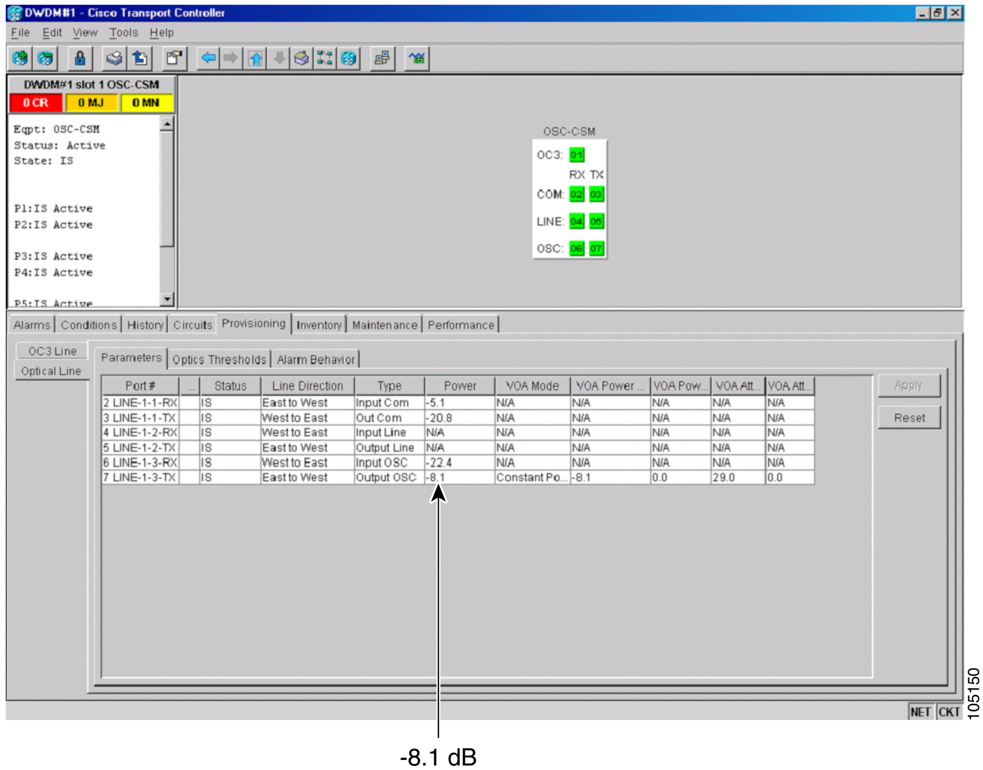
Note The OSCM cannot be used in hybrid nodes where you use OC-N cards, electrical cards, or cross-connect cards. The OSCM uses Slots 8 and 10, which are also cross-connect card slots. The OSC-CSM card is recommended for hybrid node configurations.

Figure 7-1 Inventory Window



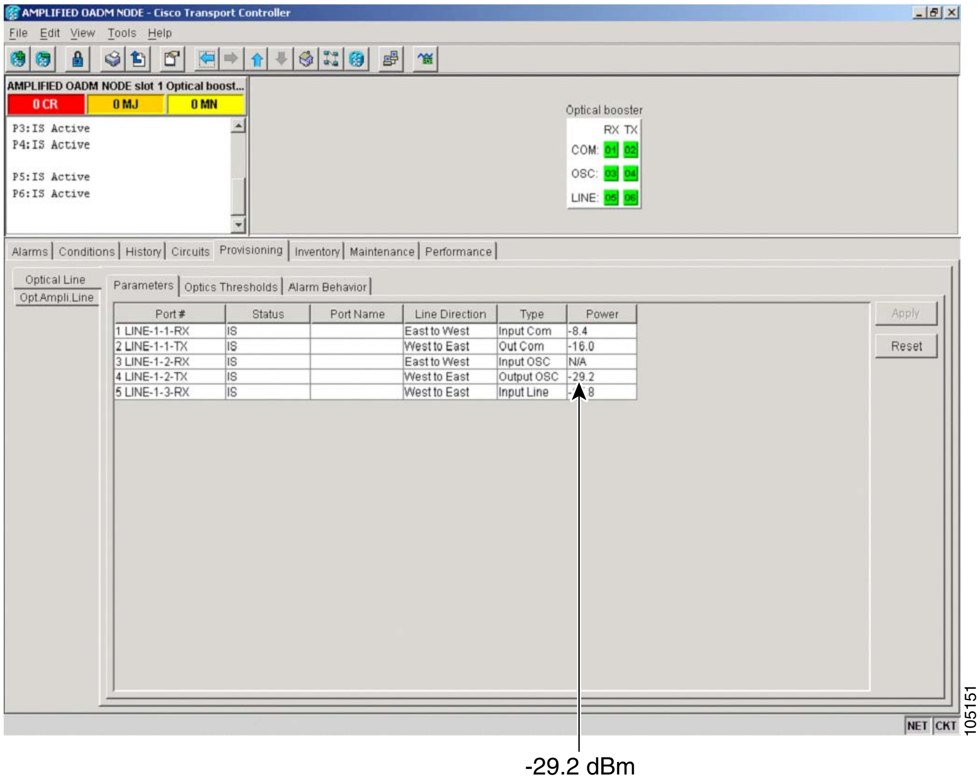
- To read the transmit power on an OSC-CSM card at the beginning of the span, in node view double-click the OSC-CSM card and click the **Provisioning > Optical Line** tabs. Read the Output OSC power value listed in the Power field for the row labeled as 7 LINE-X-3-TX where X equals the slot number (Figure 7-2).

Figure 7-2 OSC-CSM Window



- To read the received power at the end of the span when you are using an OPT-BST amplifier card, double-click the OPT-BST card and go to the OSC Tx port. Click the **Provisioning > Optical Line** tabs and read the Output OSC power value listed in the Power field for the row labeled as 4 LINE-X-2-TX where X equals the slot number (Figure 7-3). Click the **Inventory** tab and find the row labeled IL04(LINE RX->OSC TX). Make note of the insertion loss listed in the Value field. Subtract this OPT-BST insertion loss from the Output OSC power level.

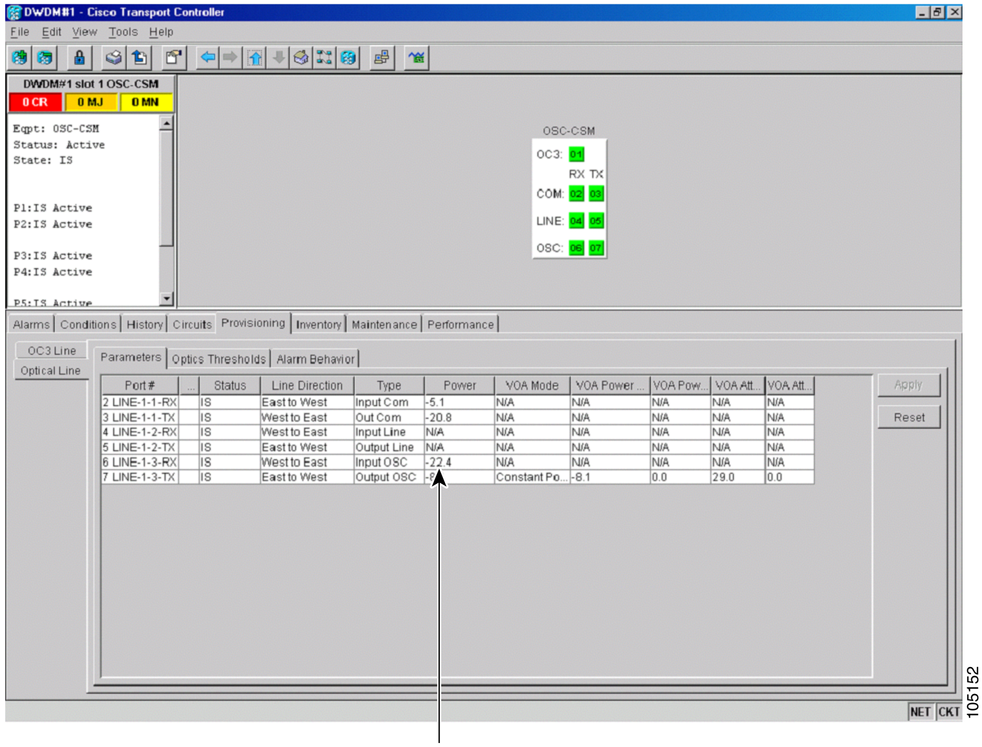
Figure 7-3 Optical Booster Window



Port #	Status	Port Name	Line Direction	Type	Power
1 LINE-1-1-RX	IS		East to West	Input Com	-8.4
2 LINE-1-1-TX	IS		West to East	Out Com	-16.0
3 LINE-1-2-RX	IS		East to West	Input OSC	N/A
4 LINE-1-2-TX	IS		West to East	Output OSC	-29.2
5 LINE-1-3-RX	IS		West to East	Input Line	-[illegible]8

- To read the received power on an OSC-CSM card, double-click the OSC-CSM card in node view to open the card view. Click the **Provisioning > Optical Line** tabs and read the Input OSC power value listed in the Power field for the row labeled as 6 LINE-X-3-RX where X equals the slot number (Figure 7-4).

Figure 7-4 OSC-CSM Window



Step 2 (Optional) If the calculated span attenuation values are not consistent with the values in the MetroPlanner file, check the fiber connection between the line Tx port and the connector at each end of the span. Also check the fiber connection between the OSCM card and the OPT-BST amplifier and repeat Step 1.

Step 3 (Optional) If the calculated span attenuation values are still not consistent, clean the fiber connectors. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21. After you have cleaned the fiber connectors, repeat Step 1.

Step 4 Return to your originating procedure (NTP).

DLP-A345 Provision the Ring ID

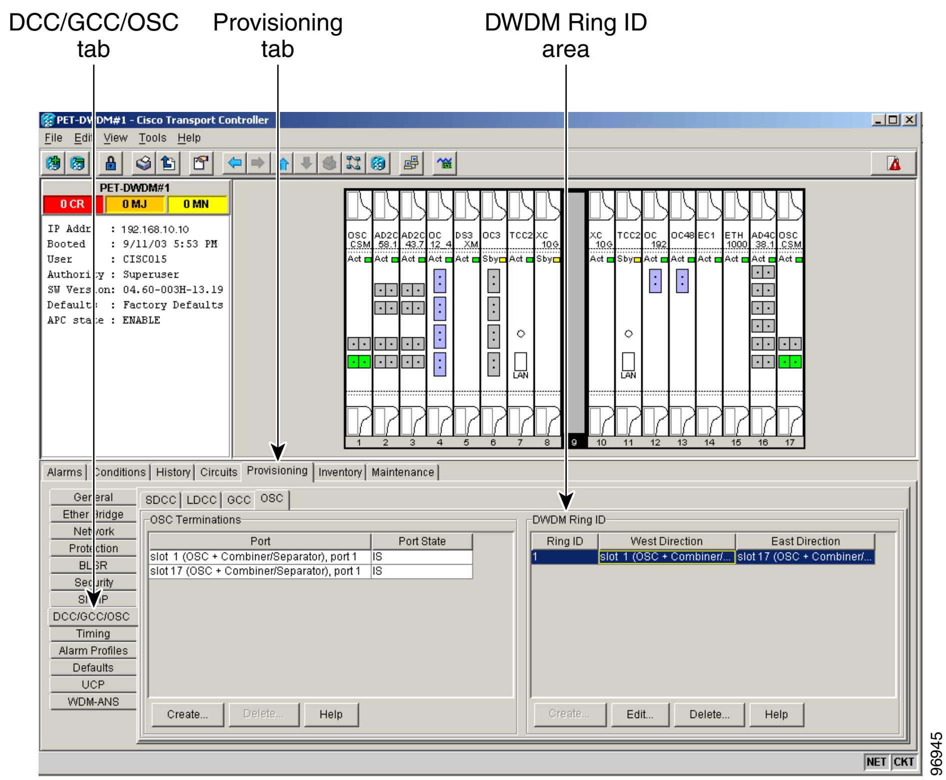
Purpose	This task creates a DWDM ring ID.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > DCC/GCC/OSC** tabs.

Step 2 Click the **OSC** tab.

Step 3 In the DWDM Ring ID area, click **Create** (Figure 7-5).

Figure 7-5 DWDM Ring ID



Step 4 In the DWDM Ring ID dialog box, enter the following information:

- Ring ID—Enter the same ID for all nodes on the ring. Choose a number from 1 to 255.
- West Line—Select a card from the drop-down menu. Selectable cards are OSCM or OSC-CSM. Slots 1 through 8 represent the west-side of the node.
- East Line—Select a card from the drop-down menu. Selectable cards are OSCM or OSC-CSM. Slots 10 through 17 represent the east-side of the node.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

NTP-A281 Provision and Verify a DWDM Network

Purpose	This procedure verifies the performance of all cable connections and cards in a network topology. You can also use this procedure to troubleshoot any problems with DWDM network set up. For information about hybrid or DWDM topologies, refer to the "DWDM Topologies" chapter in the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	Test set or protocol analyzer
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 to log into an ONS 15454 on the network.

Step 2 Review the MetroPlanner file and determine the first channel (ITU wavelength) to be provisioned. Use the transponder, muxponder, or line card that corresponds to the selected wavelength.

> **Note** Provision and measure only one channel.

Step 3 Configure the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, or line card according to the MetroPlanner file or according to your site plan. For provisioning information see the following:

- NTP-A206 Modify Line Settings and PM Parameter Thresholds for TXP_MR_10G Cards, page 13-28
- NTP-A207 Modify Line Settings and PM Parameter Thresholds for MXP_2.5G_10G Cards, page 13-37
- NTP-A237 Modify Line Settings and PM Parameter Thresholds for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-46

Step 4 If you are using cards with tunable optical wavelengths on the output port, in node view click the **Provisioning > Line > Wavelength** tabs and select the ITU wavelength according to your site plan. For TXP_MR_10G cards see the "DLP-A274 Change Card Settings for TXP_MR_10G Cards" task on page 13-29.

Step 5 Create the optical channels according to your site plan. Complete the "NTP-A227 Provision a DWDM Optical Channel Network Connection" procedure on page 8-98.

> **Note** The amplifiers automatically calculate the optical output power to maintain a constant power level on each channel every time a channel is created on the DWDM network. Automatic power control (APC) also starts every 60 minutes. If the span length changes, APC modifies amplifier gains and express variable optical attenuation (VOA). For more information about APC, refer to the "DWDM Topologies" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 6 If OPT-PRE amplifiers are being turned up for the first time:

a. In node view, double-click the OPT-PRE card to open card view.

b. Click the **Provisioning > Opt. Ampli. Line > Parameters** tabs.

c. The Power field on amplifier port #2 must reach the provisioned set point shown in the Power Ref. field. The value reported by CTC includes ASE power. These values must be consistent within plus or minus 1 dB.

d. For each OPT-PRE amplifier that is turned up for the first time on your network, repeat Steps a through c.

Step 7 If OPT-BST amplifiers are being turned up for the first time:

a. In node view, double-click the OPT-BST card to open card view.

b. Click the **Provisioning > Opt. Ampli. Line > Parameters** tabs.

c. The Power field on amplifier port #6 must reach the provisioned set point shown in the Power Ref. field. The value reported by CTC includes ASE power. These values must be consistent within plus or minus 1 dB.

d. Verify that the amplifiers have switched to constant gain mode. The amplifiers automatically calculate their gain and then switch to constant gain mode.

e. For each OPT-BST amplifier that is turned up for the first time on your network, repeat Steps a through d.

Step 8 If OADM nodes have a new circuit running traffic for the first time, check the power values:

Note This step checks the Pin OADM Stage value and the Pout OADM Stage value that characterize every OADM Node. The APC tool use these values make all of the VOA adjustments.

- If the circuit is terminated inside the node, go to node view and click the **Provisioning > WDM-ANS > Provisioning** tabs. In the OADM West Side pane, check the Pin OADM Stage value. It should match the value for the first OADM card in your circuit heading west to east shown in the COM RX port, plus or minus 2 dB. If the values are outside of the error margins, contact Cisco qualified personnel to create another MetroPlanner file or refer to the next level of support.
- If the circuit passes through the node, go to node view and click the **Provisioning > WDM-ANS > Provisioning** tabs. In the OADM West Side pane, check the Pin OADM Stage value. It should match the value for the first OADM card in your circuit heading west to east shown in the COM RX port, plus or minus 2 dB. In the OADM East Side pane, check the Pout OADM Stage value. It should match the value for the first OADM card in your circuit heading west to east shown in the COM TX port, plus or minus 1 dB. If the values are outside of the error margins, contact Cisco qualified personnel to create another MetroPlanner file or refer to the next level of support.
- If the circuit starts from the node, go to node view and click the **Provisioning > WDM-ANS > Provisioning** tabs. In the OADM East Side pane, check the Pout OADM Stage value. It should match the value for the first OADM card in your circuit heading west to east shown in the COM TX port, plus or minus 1 dB. If the values are outside of the error margins, contact Cisco qualified personnel to create another MetroPlanner file or refer to the next level of support.

Step 9 Check the received power range:

a. Complete the "DLP-A349 Clear Selected PM Counts" task on page 10-8 for the transponder, muxponder, or line card.

b. Click the **Optics PM** tab.

c. Read and make note of the values shown in the RX Optical Pwr (Min, dBm) and RX Optical Pwr (Max, dBm) fields.

d. Click the **Provisioning > Optics Thresholds** tabs.

e. Compare the values shown in Step c with the values listed in the RX Power High and RX Power Low columns. Check that the received power on the transponder, muxponder, or line card is within the allowed receiving range according to optical card sensitivity specifications. See the *Cisco ONS 15454 Reference Manual* for information about card specifications.

Step 10 Perform a short-term BER test:

a. Complete the "DLP-A349 Clear Selected PM Counts" task on page 10-8 for the transponder, muxponder, or line card.

b. Click the **Payload PM** tab, or if OTN is provisioned click the **OTN PM** tab.

c. Perform a short-term BER test using a test set or protocol analyzer.

Note To see an accurate performance monitoring count, the BER test results must be consistent with the transmitted bit rate for at least 10 minutes.

Note For information about using a test set or protocol analyzer, refer to the test set or protocol analyzer user guide.

Step 11 Repeat Steps 2 through 10 for each channel in your site plan.

Step 12 (Optional) If you have DWDM cards on nodes in your network, complete the "DLP-A346 Verify DWDM Card Parameters" task on page 7-13.

Step 13 Complete the "DLP-A497 DWDM Node Acceptance Test" task on page 7-17.

Stop. You have completed this procedure.

DLP-A346 Verify DWDM Card Parameters

Purpose	This task checks start of life (SOL) network conditions on DWDM cards. This procedure is recommended, but it is not mandatory.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 If OPT-BST amplifiers are used, retrieve parameters for each OPT-BST amplifier on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first OPT-BST amplifier to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the Power field, check the power values for Output COM, port #2 and Output OSC, port #4.

d. Click the **Opt. Ampli. Line > Parameters** tabs.

e. In the Power field, check the power value for Output Line, port #6.

f. In the Mode field, check the value for Output Line, port #6.

g. In the Gain field, check the value for Output Line, port #6.

h. In the Tilt Reference field, check the value for Output Line, port #6.

i. Click the **Maintenance > ALS** tabs and verify that the ALS Mode column displays Auto Restart. Auto Restart is the default Automatic Laser Shutdown (ALS) mode.

j. Repeat Steps a through i for each OPT-BST amplifier.

Step 3 If OPT-PRE amplifiers are used, retrieve parameters for each OPT-PRE amplifier on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first OPT-PRE amplifier to open it in card view.

b. Click the **Provisioning > Opt. Ampli. Line > Parameters** tabs.

c. In the Power field, check the power value for Output COM, port #2.

d. In the Mode field, check the value for Output COM, port #2.

e. In the Gain field, check the value for Output COM, port #2.

f. In the Tilt Reference field, check the value for Output COM, port #2.

g. In the DCU Insertion Loss field, check the value for Output COM, port #2.

h. Click the **Maintenance > ALS** tabs and verify that the ALS Mode column displays Auto Restart. Auto Restart is the default ALS mode.

i. Repeat Steps a through h for each OPT-PRE amplifier.

Step 4 If 32 MUX-O cards are used, retrieve parameters for each 32 MUX-O card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first 32 MUX-O card to open it in card view.

b. Click the **Provisioning > Optical Chn > Parameters** tabs.

c. In the Power field, check the value for Add ports 1 through 32.

d. In the VOA Attenuation Ref. field, check the value for Add ports 1 through 32.

e. Repeat Steps a through d for each 32 MUX-O card.

Step 5 If 32 DMX-O cards are used, retrieve parameters for each 32 DMX-O card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first 32 DMX-O card to open it in card view.

b. Click the **Provisioning > Optical Chn > Parameters** tabs.

c. In the Power field, check the value for Drop ports 1 through 32.

d. In the VOA Attenuation Ref. field, check the value for Drop ports 1 through 32.

e. Repeat Steps a through d for each 32 DMX-O card.

Step 6 If AD-4B-xx.x cards are used, retrieve parameters for each AD-4B-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first AD-4B-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #10.

d. Click the **Optical Band > Parameters** tabs.

e. In the Power field, check the values for the even numbered ports 2 through 8.

f. In the VOA Attenuation Ref. field, check the values for the even numbered ports 2 through 8.

g. In the Power field, check the values for the odd numbered ports 1 through 7.

h. Repeat Steps a through g for each AD-4B-xx.x card.

Step 7 If AD-1B-xx.x cards are used, retrieve parameters for each AD-1B-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first AD-1B-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #4.

d. Click the **Optical Band > Parameters** tabs.

e. In the Power field, check the value for Drop port #2.

f. In the VOA Attenuation Ref. field, check the value for Drop port #2.

g. In the Power field, check the value for Add port #1.

h. Repeat Steps a through g for each AD-1B-xx.x card.

Step 8 If AD-1C-xx.x cards are used, retrieve parameters for each AD-1C-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first AD-1C-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #4.

d. Click the **Optical Channel > Parameters** tabs.

e. In the Power field, check the value for Add port #1.

f. In the VOA Attenuation Ref. field, check the value for Add port #1.

g. In the Power field, check the value for Drop port #2.

h. Repeat Steps a through g for each AD-1C-xx.x card.

Step 9 If AD-2C-xx.x cards are used, retrieve parameters for each AD-2C-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first AD-2C-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #6.

d. Click the **Optical Channel > Parameters** tabs.

e. In the Power field, check the value for odd numbered Add ports 1 though 3.

f. In the VOA Attenuation Ref. field, check the value for odd numbered Add ports 1 through 3.

g. In the Power field, check the value for even numbered Drop ports 2 through 4.

h. Repeat Steps a through g for each AD-2C-xx.x card.

Step 10 If AD-4C-xx.x cards are used, retrieve parameters for each AD-4C-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first AD-4C-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #10.

d. Click the **Optical Channel > Parameters** tabs.

e. In the Power field, check the value for odd numbered Add ports 1 though 7.

f. In the VOA Attenuation Ref. field, check the value for odd numbered Add ports 1 through 7.

g. In the Power field, check the value for even numbered Drop ports 2 through 8.

h. In the VOA Attenuation Ref. field, check the value for even numbered Add ports 2 through 8.

i. Repeat Steps a through h for each AD-4C-xx.x card.

Step 11 If 4MD-xx.x cards are used, retrieve parameters for each 4MD-xx.x card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first 4MD-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the VOA Attenuation Ref. field, check the value for output express port #10.

d. Click the **Optical Channel > Parameters** tabs.

e. In the Power field, check the value for odd numbered Add ports 1 though 7.

f. In the VOA Attenuation Ref. field, check the value for odd numbered Add ports 1 through 7.

g. In the Power field, check the value for even numbered Drop ports 2 through 8.

h. In the VOA Attenuation Ref. field, check the value for even numbered Add ports 2 through 8.

i. Repeat Steps a through h for each 4MD-xx.x card.

Step 12 If OSC-CSM cards are used, retrieve parameters for each OSC-CSM card on the network and compare the values with the values in MetroPlanner if available:

a. In node view double-click the first OSC-CSM card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the Power field, check the value for output COM port #3.

d. In the Power field, check the value for input OSC port #6.

e. In the Power field, check the value for output OSC port #7.

f. In the VOA Attenuation Ref. field, check the value for output OSC port #7.

g. Click the **Maintenance > ALS** tabs and verify that the ALS Mode column displays Auto Restart. Auto Restart is the default ALS mode.

h. Repeat Steps a through g for each OSC-CSM card.

Step 13 If OSCM cards are used, retrieve parameters for each OSCM card on the network and compare the values with the values in MetroPlanner if available:

Note The OSCM cannot be used in hybrid nodes where you use OC-N cards, electrical cards, or cross-connect cards. The OSCM uses Slots 8 and 10, which are also cross-connect card slots. The OSC-CSM card is recommended for hybrid node configurations.

a. In node view double-click the first OSCM card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the Power field, check the value for output OSC port #3.

d. In the VOA Attenuation Ref. field, check the value for output OSC port #3.

e. Click the **Maintenance > ALS** tabs and verify that the ALS Mode column displays Auto Restart. Auto Restart is the default ALS mode.

f. Repeat Steps a through e for each OSCM card.

Step 14 If AD-xx-xx.x cards are used, look at the first and the last card along a defined direction such as west to east.

a. In node view double-click the first AD-xx-xx.x card to open it in card view.

b. Click the **Provisioning > Optical Line > Parameters** tabs.

c. In the Power field, check the value for input COM port x.

d. Go to card view for the last AD-xx-xx.x card and click the **Provisioning > Optical Line > Parameters** tabs.

e. In the Power field, check the value for output COM port y.

f. Repeat Steps a through e for each direction. For example if you performed the procedure from west to east, now perform the procedure from east to west.

Step 15 Return to your originating procedure (NTP).

DLP-A497 DWDM Node Acceptance Test

Purpose	This task tests each node in a network topology.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Alarms** tab:

a. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

b. Complete the "DLP-A516 Export CTC Data" task on page 9-4 to export alarm and condition information.

c. Verify that the alarm filter is not turned on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

d. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service.

Step 4 Return to your originating procedure (NTP).

NTP-A282 Verify the Optical Receive Power

Purpose	This procedure verifies the optical receive power.
Tools/Equipment	Optical power meter
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at an ONS 15454 on the network.

Step 2 Using an optical power meter, check the receive optical power on both ends of the span:

a. Identify a transmit port on an AD-xC-xx.x card or a 32 DMX-O card in the node that you want to test and connect it to the optical power meter.

b. Read the values displayed on the optical power meter. These values must be consistent with the data provided by the MetroPlanner installation file, plus or minus 1 dB. To view MetroPlanner values click the **Provisioning > WDM-ANS > Provisioning** tabs. The values are listed in the Pdrop field for demux cards and in the Pout Band field for OADM cards.

Note For information about using an optical power meter, refer to the optical power meter user guide.

Step 3 If the optical power is too low, check the fiber connections as appropriate to your node configuration:

- Check the fiber connections between the OPT-BST amplifier or the OSC-CSM card and the OPT-PRE amplifier or the next OADM card.
- Check the fiber connections between the OADM cards and if needed clean the connectors. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21.

Step 4 If the power coming from the AD-xC-xx.x card is higher than required, put an external optical attenuator before the client interface input in order to meet the power requirement.

Step 5 If the power coming from the 32 DMX-O card is higher or lower than required, you can regulate the VOA in CTC.

- From the 32 DMX-O card view, choose the **Provisioning > Optical Chn > Parameters** tabs. The VOA columns including the VOA power and attenuation reference points can be manually set according to your site plan.
- Changing the VOA power and attenuation calibration values adjusts the power and attenuation reference settings.

Stop. You have completed this procedure.

NTP-A283 Verify the OSNR

Purpose	This procedure verifies the optical signal-to-noise ratio (OSNR). OSNR is the ratio between the signal power level and the noise power level.
Tools/Equipment	Optical spectrum analyzer
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at an ONS 15454 on the network.

Step 2 Using an optical spectrum analyzer, check the received OSNR for each transmitted channel on both ends of the span:

a. Identify the LINE Rx monitor port on an OPT-PRE amplifier (MON Rx) or OSC-CSM card (MON Rx) in the node that you want to test and connect it to the optical spectrum analyzer.

b. Calculate the OSNR values, based on the optical spectrum retrieved. These values must be consistent with the data provided by the MetroPlanner installation file, plus or minus 1 dB. The OSNR values in the MetroPlanner file are only valid for the Rx locations of a dropped channel. Therefore, OSNR values of an expressed channel at an OADM cannot be compared to the MetroPlanner values.

Note For information about using a spectrum analyzer, refer to the spectrum analyzer user guide.

Note For OSNR values for each card class, refer to the "DWDM Cards" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 3 If the OSNR is too low, check the following depending on your node configuration:

Note The purpose of this step is not to improve the signal-to-noise ratio (SNR), but to match the per channel power level within the receive (Rx) port power range.

- Check the fiber connections between the OPT-BST amplifier or the OSC-CSM and the OPT-PRE amplifier and if needed clean the connectors. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21.
- On the near-end OPT-BST amplifier, check the equalization of the added channels at the monitor output.
- On the OPT-PRE amplifier, check the output power on both COM-Tx and DC-Tx ports.
- On the far-end OPT-PRE amplifier, check the amplifier gain tilt at the monitor output.

Stop. You have completed this procedure.

NTP-A284 Convert a Pass-Through Connection to an Add/Drop Connection

Purpose	This procedure converts a pass-through connection to two add or drop connections (one on the add side and the other on the drop side). Use this procedure during a network upgrade. Pass-through channel connections can be provided between channel input and output ports for the AD-xC-xx.x, the 4MD-xx.x, the 32 MUX-O, and the 32 DMX-O. You can set up pass-through connections in nodes that might require more add or drop channel capability or configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at an ONS 15454 on the network.

Step 2 In node view click the **Circuits** tab. Delete the unidirectional or bidirectional pass-through OCHNC that applies to the pass-through connection to be removed.

Step 3 Remove the physical pass-through cabling. Click the **Provisioning > WDM-ANS > Connections** tabs to identify the card ports to be removed. The pass through connection you are removing can be connected in both OADM and HUB nodes.

- For a hub node—Connect the 32 DMX-O output port to the 32 MUX-O input port.
- For an OADM node—Connect the AD-xC-xx.x drop (output) port to the AD-xC-xx.x add (input) port.

Step 4 Physically connect the proper client interface to the correct ADD and DROP ports.

Step 5 Delete the filter connections related to the pass-through connection that is being converted to an add/drop connection:

a. In node view, click the **Provisioning > WDM-ANS > Port Status** tabs.

b. Highlight the pass-through connections between ITU channel add and drop ports on filters.

c. Click **Delete**.

Step 6 Create two new unidirectional OCHNCs (one heading east, the other heading west) to support the new add/drop channels. See the "NTP-A227 Provision a DWDM Optical Channel Network Connection" procedure on page 8-98.

Step 7 If it is necessary, add an optical attenuator between the Channel-Tx port of the OADM card, 4MD-xx.x card, or the 32 DMX-O card and the DWDM-Rx port on the transponder, muxponder, or line card.

Note If the channel is coming from a 32 DMX-O, the optical power can be adjusted in CTC by modifying the value of the internal per channel VOA.

Step 8 (Optional) The following verification steps might be needed for an intermediate node when a pass-through connection is converted:

- Verify that the received channels are at the specified power level. See the "NTP-A282 Verify the Optical Receive Power" procedure on page 7-18 for instructions.
- Verify that the added channels are equalized with the express channels within 1 dB.
- If the channels are not equalized with the express channels within plus or minus 1 dB, check the attenuation of the VOAs.
- Also check all the fiber adapters to minimize their insertion losses. See the "NTP-A112 Clean Fiber Connectors" procedure on page 17-21 for instructions.

Stop. You have completed this procedure.

Create Circuits and VT Tunnels

This chapter explains how to create Cisco ONS 15454 electrical circuits, tunnels, OC-N circuits, Ethernet circuits, dense wavelength division multiplexing (DWDM) optical channel network connections, and virtual concatenated (VCAT) circuits. For additional information about ONS 15454 circuits, refer to the “Circuits and Tunnels” chapter in the *Cisco ONS 15454 Reference 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.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

12. NTP-A188 Create an Automatically Routed OC-N Circuit, page 8-42—Complete as needed.
13. NTP-A189 Create a Manually Routed OC-N Circuit, page 8-47—Complete as needed.
14. NTP-A190 Create a Unidirectional OC-N Circuit with Multiple Drops, page 8-51—Complete as needed.
15. NTP-A62 Test OC-N Circuits, page 8-54—Complete this procedure after you create an optical (OC-N) circuit.
16. NTP-A139 Create a Half Circuit on a BLSR or 1+1 Node, page 8-56—Complete this procedure as needed to create a half circuit using an OC-N as a destination in a bidirectional line switched ring (BLSR) or 1+1 topology.
17. NTP-A140 Create a Half Circuit on a Path Protection Node, page 8-58—Complete as needed to create a half circuit using an OC-N as a destination in a path protection.
18. NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 8-61—Complete as needed.
19. NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 8-68—Complete as needed.
20. NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 8-70—Complete as needed.
21. NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration, page 8-73—Complete as needed.
22. NTP-A144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect, page 8-75—Complete as needed.
23. NTP-A145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect, page 8-77—Complete as needed.
24. NTP-A146 Test E-Series Circuits, page 8-81—Complete this procedure after creating E-Series SONET circuits.
25. NTP-A147 Create a G-Series STS Circuit, page 8-82—Complete as needed.
26. NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode, page 8-84—Complete as needed.
27. NTP-A241 Provision G-Series Ports for Transponder Mode, page 8-88—Complete as needed.
28. NTP-A149 Test G-Series Circuits, page 8-91—Complete this procedure after creating G-Series SONET circuits.
29. NTP-A194 Create Overhead Circuits, page 8-93—Complete as needed to create data communications channel (DCC) tunnels or IP-encapsulated tunnels, provision orderwire, or create user data channel circuits.
30. NTP-A227 Provision a DWDM Optical Channel Network Connection, page 8-98—Complete as needed.
31. NTP-A264 Create an Automatically Routed VCAT Circuit, page 8-99—Complete as needed.
32. NTP-A265 Create a Manually Routed VCAT Circuit, page 8-103—Complete as needed.

Table 8-1 defines ONS 15454 circuit creation terms and options.

Table 8-1 ONS 15454 Circuit Options

Circuit Option	Description
Source	The circuit source is where the circuit enters the ONS 15454 network.
Destination	The circuit destination is where the circuit exits an ONS 15454 network.
Automatic circuit routing	Cisco Transport Controller (CTC) routes the circuit automatically on the shortest available path based on routing parameters and bandwidth availability.
Manual circuit routing	Manual routing allows you to choose a specific path, not just the shortest path chosen by automatic routing. You can choose a specific synchronous transport signal (STS) or virtual tributary (VT) for each circuit segment and create circuits from work orders prepared by an operations support system (OSS) like the Telcordia Trunk Information Record Keeping System (TIRKS).
VT tunnel	VT tunnels allow VT1.5 circuits to pass through an ONS 15454 without utilizing cross-connect card (XC, XCVT, XC10G) resources. VT circuits using VT tunnels use cross-connect capacity only at the source and destination nodes. One VT tunnel can carry 28 VT1.5 circuits.
VT aggregation point	VT aggregation points (VAPs) allow VT circuits to be aggregated into an STS for handoff to non-ONS 15454 networks or equipment, such as interoffice facilities (IOFs), switches, or digital access cross-connect systems. VAPs reduce VT matrix resource utilization at the node where the VT1.5s are aggregated onto the STS. This node is called the STS grooming end. The STS grooming end requires an OC-N, EC-1, or DS3XM-6 card. VT aggregation points can be created on BLSR, 1+1, or unprotected nodes, but cannot be created on path protection nodes.

ONS 15454 circuits are either VT or STS circuits. Table 8-2 shows the circuit source and destination options for VT circuits.

Table 8-2 CTC Circuit Source and Destination Options for VT Circuits

Card	Ports	STSs	VTs	DS1s
DS1-14, DS1N-14	—	—	—	14
DS3XM-6	6	—	—	28 per port
EC1-12	12	—	28 per port	—
OC3 IR 4/STM1 SH 1310	4	3 per port	28 per STS	—
OC3 IR/STM1 SH 1310-8	8	3 per port	28 per STS	—
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12	28 per STS	—
OC12 IR/STM4 SH 1310-4	4	12 per port	28 per STS	—
All OC-48 cards (does not include the ML-Series card)	—	48	28 per STS	—
All OC-192 cards	—	192	28 per STS	—
FC_MC-4[1]	4	—	—	—

1. For contiguous concatenated (CCAT) circuits, the FC_MC-4 card maps STS-24c or STS-48c to a port. For VCAT, the FC_MC-4 card maps STS3c-8v to a port.

Table 8-3 shows the shows the circuit source and destination options for STS circuits.

Table 8-3 CTC Circuit Source and Destination Options for STS Circuits

Card	Ports	STSs
DS1-14, DS1N-14[1]	—	—
DS3-12, DS3N-12, DS3-12E, DS3N-12E	12	—
DS3XM-6	6	—
DS3I-N-12	12	1 per port
EC1-12	12	—
OC3 IR 4/STM1	4	3 per port
OC3-8	8	3 per port
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12
OC12 IR/STM4 SH 1310-4	4	12 per port
All OC-48 cards (includes ML-Series card)	—	48
All OC-192 cards	—	192
FC_MC-4[2]	4	—

1. You can route one STS circuit on a DS-1 card to carry all 14 ports within the STS. However, 14 VT1.5s are not utilized.
2. For CCAT circuits, the FC_MC-4 card maps STS-24c or STS-48c to a port. For VCAT, the FC_MC-4 card maps STS3c-8v to a port.

NTP-A127 Verify Network Turn Up

Purpose	This procedure verifies that the ONS 15454 network is ready for circuit provisioning.
Tools/Equipment	None
Prerequisite Procedures	Chapter 6, "Turn Up Network"
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**. Wait for all the nodes that are part of the network to appear on the network map. (Large networks might take several minutes to display all the nodes.)

> **Note** If this is the first time your computer has connected to this ONS 15454 network, the node icons are stacked on the left side of the graphic area, possibly out of view. Use the scroll bar under the network map to display the icons. To separate the icons press **Ctrl** and drag and drop the icon to the new location. Repeat until all the nodes are visible on the graphic area.

Step 3 Verify node accessibility. In the network view, all node icons must be either green, yellow, orange, or red.

If all network nodes do not appear after a few minutes, or if a node icon is gray with an IP address under it, do not continue. Look at the Net box in the lower right corner of the window. If it is gray, log in again, making sure not to check the Disable Network check box in the CTC Login dialog box. If problems persist, see Chapter 6, "Turn Up Network" to review the network turn-up procedure appropriate for your network topology, or refer to the *Cisco ONS 15454 Troubleshooting Guide* for troubleshooting procedures.

Step 4 Verify DCC connectivity. All nodes must be connected by green lines. If lines are missing or gray in color, do not continue. See Chapter 6, "Turn Up Network" and follow the network turn-up procedure appropriate for your network topology. Verify that all nodes have DCC connectivity before continuing.

Step 5 Click the **Alarms** tab to view alarm descriptions. Investigate and resolve, if necessary, all critical (red node icon) or major (orange node icon) alarms. Refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve alarms before continuing.

Step 6 From the View menu, choose **Go to Home View**. Verify that the node is provisioned according to your site or engineering plan:

a. View the cards in the shelf map. Verify that the ONS 15454 cards appear in the specified slots.

b. Click the **Provisioning > General** tabs. Verify that the node name, contacts, date, time, and Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server IP address (if used) are correctly provisioned. If needed, make corrections using the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-7.

c. Click the **Network** tab. Verify that the IP address, Subnet Mask, Default Router, Prevent LCD IP Config, and Gateway Settings are correctly provisioned. If not, make corrections using the "NTP-A169 Set Up CTC Network Access" procedure on page 4-9.

d. Click the **Protection** tab. Verify that protection groups are created as specified in your site plan. If the protection groups are not created, complete the "NTP-A170 Create Protection Groups" procedure on page 4-26.

e. If the node is in a BLSR, click the **BLSR** tab. (If the node is not in a BLSR, continue with Step f.) Verify that the following items are provisioned as specified in your site plan:

- BLSR type (2-fiber or 4-fiber)
- BLSR ring ID and node IDs
- Ring reversion time
- East and west card assignments
- 4-fiber BLSRs: span reversion and east/west protect card assignments

If you need to make corrections, see the "NTP-A40 Provision BLSR Nodes" procedure on page 6-15 for instructions.

f. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-A30 Create Users and Assign Security" procedure on page 4-4 to correct the information.

g. If simple network management protocol (SNMP) is used, click the **SNMP** tab and verify the trap and destination information. If the information is not correct, see the "NTP-A87 Change SNMP Settings" procedure on page 12-33 to correct the information.

h. Click the **DCC/GCC/OSC** tab. Verify that DCCs were created to the applicable OC-N slots and ports (time-division multiplexing [TDM] nodes) or Optical Service Channel (OSC) slots and ports (DWDM nodes). If DCCs were not created for the appropriate OC-N or OSC slots and ports, see Chapter 6, "Turn Up Network" and complete the turn-up procedure appropriate for your network topology.

i. Click the **Timing** tab. Verify that timing is provisioned as specified. If not, use the "NTP-A85 Change Node Timing" procedure on page 12-23 to make the changes.

j. Click the **Alarm Profiles** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-A71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 9-17 to change the information.

k. Verify that the network element defaults listed in the status area of the node view window are correct.

Step 7 Repeat Step 6 for each node in the network.

Step 8 Complete the appropriate circuit creation procedure from the NTP list in the "NoteThe 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." section on page 8-1.

Stop. You have completed this procedure.

NTP-A181 Create an Automatically Routed DS-1 Circuit

Purpose	This procedure creates an automatically routed DS-1 circuit, meaning that CTC chooses the circuit route based on the parameters you specify and on the software version. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network.

- Number of Circuits—Type the number of DS-1 circuits you want to create. The default is 1. If you are creating multiple circuits with the same slot and sequential port numbers, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This check box is automatically selected if you enter more than 1 in the Number of Circuits field. Auto-ranging creates identical (same source and destination) sequential circuits automatically. Uncheck the box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-1):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

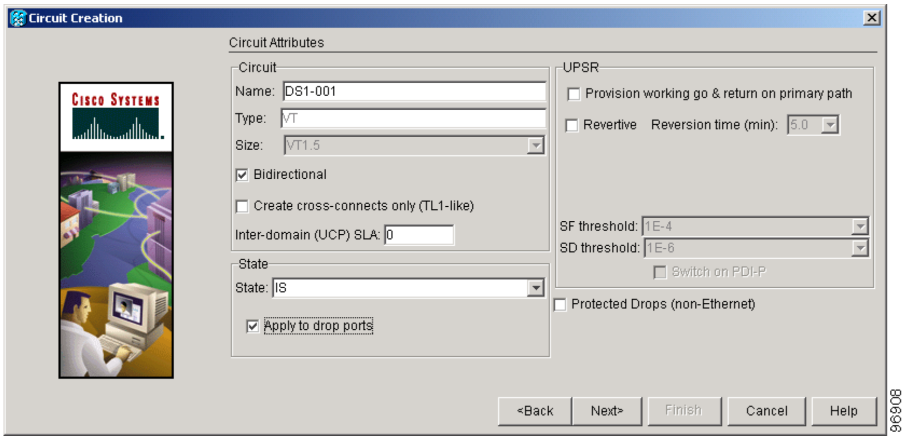
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms are generated if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement (SLA) number. Otherwise, leave the field set to zero.

- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this box, CTC displays only protected cards and ports as source and destination choices.

Figure 8-1 Setting Circuit Attributes for a DS-1 Circuit



Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11. Otherwise, continue with the next step.

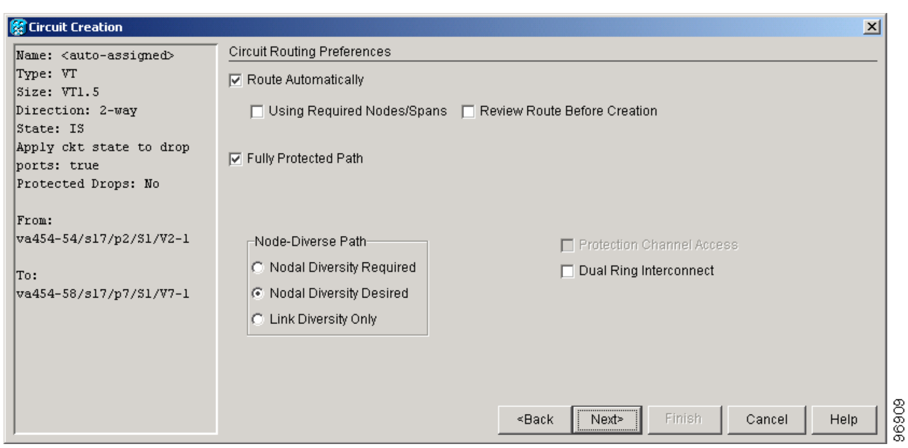
Step 9 Click **Next**.

Step 10 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 8-12.

Step 11 In the Circuit Routing Preferences area (Figure 8-2), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box if you want to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.

Figure 8-2 Setting Circuit Routing Preferences for a DS-1 Circuit



Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected. They are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection dual ring interconnect (DRI), check the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps. If not, continue with Step 18.

a. Click **Next**.
b. In the Circuit Route Constraints area, click a node or span on the circuit map.
c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.
d. Repeat Step c for each node or span you wish to include or exclude.
e. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 Click **Next**. In the Create area of the VT Circuit Options panel, choose one of the following:

- VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC-1, DS3XM-6, or OC-N port on a BLSR, 1+1, or unprotected node. VT aggregation points (VAPs) collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or digital access and cross-connect system (DACS). It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than

multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:

  – Circuit source is STS grooming node—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC-1, DS3XM-6, or OC-N card.
  – Circuit destination is STS grooming node—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC-1, DS3XM-6, or OC-N card.

- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 17 If you chose VT aggregation point, complete the following substeps. If not, continue with Step 18.

a. Click **Next**.

b. In the VT Aggregation Point Destination panel, click the node that you want to be the VAP destination, then click **Add Destination**.

Step 18 If you selected Review Route Before Creation in Step 11, complete the following substeps. If not, continue with Step 19.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A182 Create a Manually Routed DS-1 Circuit" procedure on page 8-13.

Step 19 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 19 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 20 In the Circuits window, verify that the new circuit(s) appear in the circuits list.

Step 21 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-A314 Assign a Name to a Port

Purpose	Use this task to assign a name to a port on any ONS 15454 card.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the card that has the port you want to provision.

Step 2 Click the **Provisioning** tab.

Step 3 Click the **Port Name** column for the port number you are assigning a name.

Step 4 Type the port name.

The port name can be up to 32 alphanumeric/special characters. The field is blank by default.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A218 Provision Path Protection Selectors During Circuit Creation

Purpose	This task provisions path protection selectors during circuit creation. Use this task only if the circuit will be routed on a path protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 The Circuit Creation wizard Circuit Attributes panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the path protection area of the Circuit Attributes panel, set the path protection path selectors:

- Provision working go and return on primary path—Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional path protection circuits.
- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.

- SF threshold—For STS circuits, set the path protection path-level signal failure bit error rate (BER) thresholds. Unavailable for VT circuits.
- SD threshold—For STS circuits, set the path protection path-level signal degrade BER thresholds. Unavailable for VT circuits.
- Switch on PDI-P—For STS circuits, check this box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for VT circuits.

Step 2 Return to your originating procedure (NTP).

DLP-A95 Provision a DS-1 Circuit Source and Destination

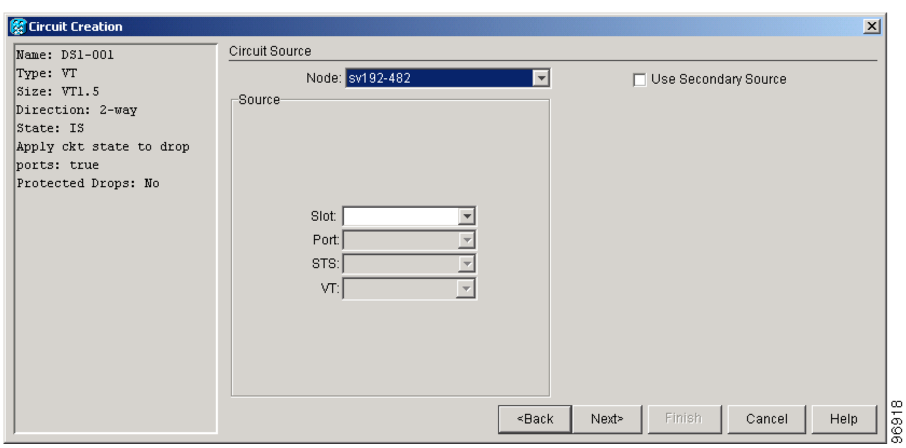
Purpose	This task provisions an electrical circuit source and destination for a DS-1 circuit. This task does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu, choose the node where the source will originate.

Step 2 From the Slot drop-down menu, choose the slot containing the DS1-14, DS1N-14, or DS3XM-6 card where the circuit will originate (Figure 8-3).

Figure 8-3 Defining the Circuit Source on a DS-1 Card



Step 3 Only if you chose DS3XM-6 as the card, choose the port from the Port drop-down menu.

Step 4 From the DS-1 drop-down menu, choose the source DS-1.

Step 5 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source. If you do not need to create a secondary source, continue with Step 6.

Step 6 Click **Next**.

Step 7 From the Node drop-down menu, choose the destination (termination) node.

Step 8 From the Slot drop-down menu, choose the slot containing the destination card. The destination is typically a DS-1 card. You can also choose an OC-N card to map the DS-1 to a VT1.5 for OC-N transport.

Step 9 Depending on the destination card, choose the destination port, STS, VT, or DS1 from the drop-down menus that appear based on the card selected in Step 8. See Table 8-2 on page 8-3 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s already used by other circuits. If another user and you working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

Step 10 If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection, click **Use Secondary Destination** and repeat Steps 7 through 9 to define the secondary destination.

Step 11 Click **Next**.

Step 12 Return to your originating procedure (NTP).

NTP-A182 Create a Manually Routed DS-1 Circuit

Purpose	This procedure creates a DS-1 circuit and allows you to provision the circuit route. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network.
- Number of Circuits—Type the number of DS-1 circuits you want to create. The default is 1.

- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in Number of Circuits.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-1 on page 8-8):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this box, CTC shows only protected cards and ports as source and destination choices.

Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 8-12.

Step 11 In the Circuit Routing Preferences area (Figure 8-2 on page 8-8), uncheck **Route Automatically**.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 17.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 17.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose a Node-Diverse Path option:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired— Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Create area of the VT Circuit Options panel, choose one of the following:

- VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC-1, DS3XM-6, or OC-N port on a BLSR, 1+1, or unprotected node. VT aggregation points (VAPs) collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - Circuit source is STS grooming node—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC-1, DS3XM-6, or OC-N card.
  - Circuit destination is STS grooming node—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC-1, DS3XM-6, or OC-N card.

- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 16 If you chose VT aggregation point, complete the following substeps. If not, continue with Step 18.

a. Click **Next**.

b. In the VT Aggregation Point Destination panel, click the node that you want to be the VAP destination, then click **Add Destination**.

Step 17 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 18 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 8-16 for the DS-1 circuit you are creating.

Step 19 Click **Finish**. CTC compares your manually provisioned circuit route with the specified path diversity option you chose in Step 13. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path. If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 19 for each additional circuit.

Step 20 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created are correct.

Step 21 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

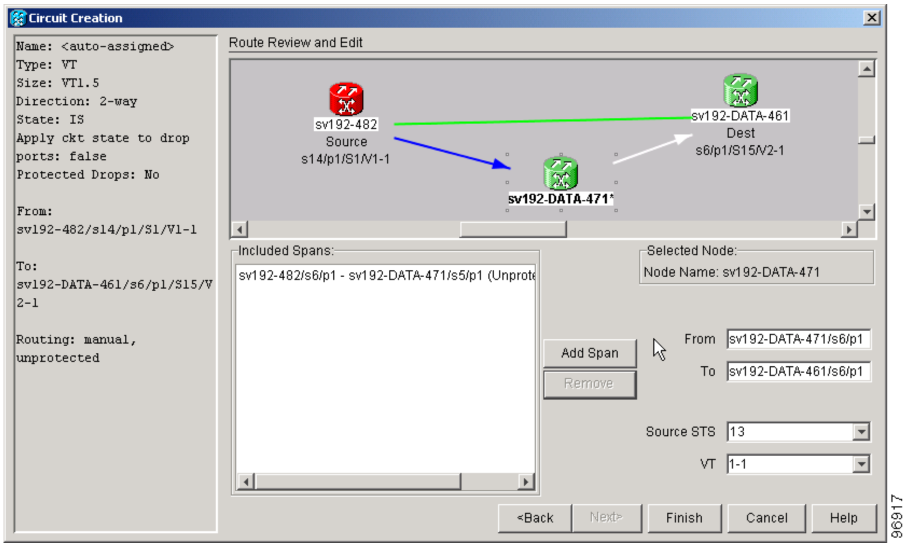
DLP-A96 Provision a DS-1 or DS-3 Circuit Route

Purpose	This task provisions the circuit route for manually routed DS-1 or DS-3 circuits. This task does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	The Circuit Creation wizard Route Review and Edit panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Route Review and Edit area of the Circuit Creation wizard, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS and VT (DS-1 circuit only) appear. Figure 8-4 shows a DS-1 circuit example.

Figure 8-4 Manually Routing a DS-1 Circuit



Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step 4.

Step 4 If you want to change the source VT for DS-1 circuits, adjust the Source VT field; otherwise, continue with Step 5.

Note VT is gray (unavailable) for DS-3 circuits.

Step 5 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 6 If the Fully Protect Path check box is checked in the Circuit Routing Preferences panel, you must:

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination. If the Dual Ring Interconnect check box is checked, you must also add bidirectional spans between the DRI nodes. To do this, click a DRI node, then double-click the arrow pointing to the adjacent DRI node to create a bidirectional span.
- Add one span for all BLSR or 1+1 portions of route from the source to the destination.

Step 7 Repeat Steps 2 through 6 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 8 Return to your originating procedure (NTP).

NTP-A183 Create a Unidirectional DS-1 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-1 circuit with multiple drops (destinations). This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **VT**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-5):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Uncheck for this circuit.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

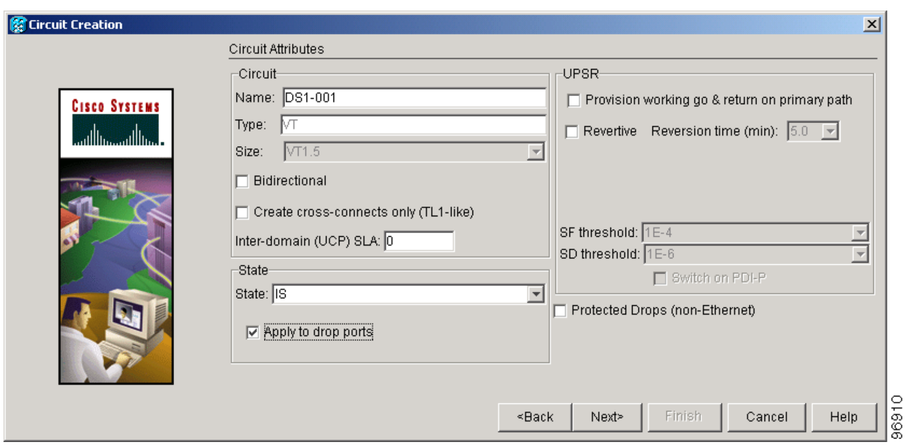
> **Note** If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

> **Note** Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this box, CTC displays only protected cards as source and destination choices.

Figure 8-5 Setting Circuit Attributes for a Unidirectional DS-1 Circuit



Step 8 Click **Next**.

Step 9 Complete the "DLP-A95 Provision a DS-1 Circuit Source and Destination" task on page 8-12.

Step 10 In the Circuit Routing Preferences area, uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 11 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 17.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 17.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 12 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 13 If you selected Fully Protected Path in Step 11 and the circuit will be routed on a path protection DRI, click the **Dual Ring Interconnect** check box.

Step 14 Click **Next**. In the Create area of the VT Circuit Options panel, choose one of the following:

- VT tunnel on transit nodes—This option is available if the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15454 Reference Manual* for more information.
- VT aggregation point—This option is available if the DS-1 circuit source or destination is on an EC-1, DS3XM-6, or OC-N port on a BLSR, 1+1, or unprotected node. VT aggregation points (VAPs) collect DS-1s on an STS for handoff to non-ONS 15454 networks or equipment, such as an IOF, switch, or DACS. It allows VT1.5 circuits to be routed through the node using one STS connection on the cross-connect card matrix rather than multiple VT connections on the cross-connect card VT matrix. If you want to aggregate the DS-1 circuit you are creating with others onto an STS for transport outside the ONS 15454 network, choose one of the following:
  - Circuit source is STS grooming node—Creates the VAP on the DS-1 circuit source node. This option is available only if the DS-1 circuit originates on an EC-1, DS3XM-6, or OC-N card.
  - Circuit destination is STS grooming node—Creates the VAP on the DS-1 circuit destination node. This option is available only if the DS-1 circuit terminates on an EC-1, DS3XM-6, or OC-N card.
- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

Step 15 If you chose VT aggregation point, complete the following substeps. If not, continue with Step 18.

a. Click **Next**.

b. In the VT Aggregation Point Destination panel, click the node that you want to be the VAP destination, then click **Add Destination**.

Step 16 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 17 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 8-16 for the DS-1 circuit you are creating.

Step 18 Click **Finish**. CTC completes the circuit and the Circuits window appears.

Step 19 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 20 Click **Edit** (or double-click the circuit row). The Edit Circuit window appears with the General tab selected.

All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. To rearrange a node icon, select the node, press **Ctrl**, then drag and drop the icon to the new location.

Step 21 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 22 Click **Create**.

Step 23 In the Define New Drop dialog box, create the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS, VT, or DS1—Choose the port, STS, VT, or DS1 from the Port, STS, VT, or DS1 drop-down menus. The card you chose in Step b determines the fields that appear. See Table 8-2 on page 8-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 12 for the option descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 11 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit State drop-down menu. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit State to the circuit source and destination drops.

g. Click **Finish**. The new drop appears in the Drops list.

Step 24 If you need to create additional drops for the circuit, repeat Steps 22 and 23 to create the additional drops.

Step 25 Click **Close**. The Circuits window appears.

Step 26 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear repeat Steps 5 through 25, making sure all options are provisioned correctly.

Step 27 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A184 Create an Automatically Routed DS-3 Circuit

Purpose	This procedure creates an automatically routed DS-3 circuit. CTC routes the circuit automatically based on circuit creation parameters and the software version. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Type the number of DS-3 circuits you want to create. The default is 1. If you are creating multiple circuits with sequential source and destination ports, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This box is automatically selected if you enter more than 1 in the Number of Circuits field. Leave selected if you are creating multiple DS-3 circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want CTC to create sequential circuits automatically.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-6):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose **STS-1**. For circuits on the DS3i-N-12 card, choose **STS-3c**. This sets a port group for ports 1, 4, 7, and 10 using 3 ports at any given time.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.

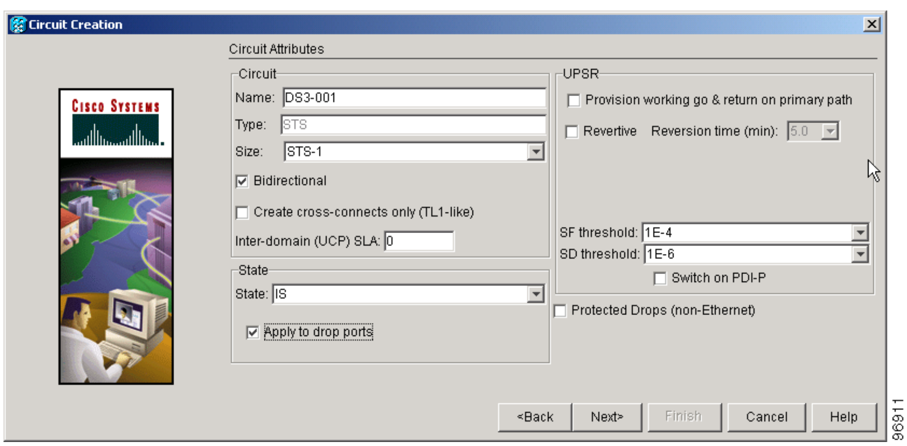
- OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
- OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this box if you want the circuit routed on protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this box, CTC provides only protected cards and ports as source and destination choices.

Figure 8-6 Setting Circuit Attributes for a DS-3 Circuit



Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

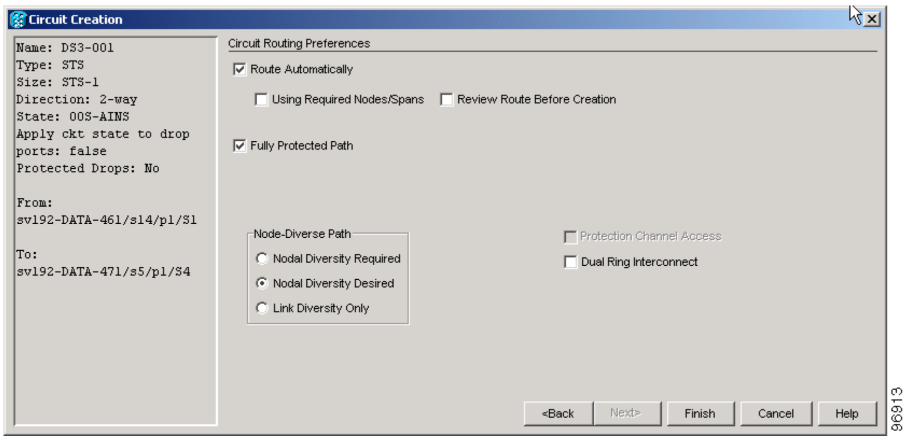
Step 9 Click **Next**.

Step 10 Complete the "DLP-A208 Provision a DS-3 Circuit Source and Destination" task on page 8-26.

Step 11 In the Circuit Routing Preferences area (Figure 8-7), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences:

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

Figure 8-7 Setting Circuit Routing Preferences for a DS-3 Circuit



Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps; otherwise, continue with Step 16:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans determines the circuit sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node from the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Note If a node or span stays gray, that node or span is required.

Step 16 If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 17.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A185 Create a Manually Routed DS-3 Circuit" procedure on page 8-27.

Step 17 Click **Finish**. One of the following actions occurs based on the circuit properties you selected:

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 18 In the Circuits window, verify that the circuit(s) you just created appear in the circuits list.

Step 19 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-A208 Provision a DS-3 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-3 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu, choose the node where the source will originate.

Step 2 From the Slot drop-down menu, choose the slot containing the DS-3 card where the circuit will originate. If you are configuring a DS-3 circuit with a transmux card, choose the DS3XM-6 card.

Step 3 From the Port drop-down menu, choose the source DS-3 or DS3XM-6 card as appropriate.

Step 4 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu, choose the destination (termination) node.

Step 7 From the Slot drop-down menu, choose the slot containing the destination card. The destination is typically a DS3XM-6 or DS-3 card. You can also choose an OC-N card to the map DS-3 circuit to an STS.

Step 8 Depending on the destination card, choose the destination port or STS from the submenus that appear based on the card selected in Step 2. See Table 8-2 on page 8-3 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s if they are already in use by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

Step 9 If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

NTP-A185 Create a Manually Routed DS-3 Circuit

Purpose	This procedure creates a DS-3 circuit and allows you to provision the circuit route. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 3.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 4.

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

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

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

- Circuit Type—Choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Type the number of DS-3 circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in Number of Circuits.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-5 on page 8-19):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave this field blank, CTC assigns a default name to the circuit.
- Size—Choose **STS-1**. For circuits on the DS3i-N-12 card, choose **STS-3c**. This sets a port group for ports 1, 4, 7, and 10 using 3 ports at any given time.
- Bidirectional—Leave this field checked (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A208 Provision a DS-3 Circuit Source and Destination" task on page 8-26.

Step 11 In the Circuit Routing Preferences area (Figure 8-7 on page 8-24), uncheck **Route Automatically**.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, click the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 8-16 for the DS-3 you are creating.

Step 17 Click **Finish**. If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created appear in the window.

Step 19 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A186 Create a Unidirectional DS-3 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-3 circuit with multiple drops. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

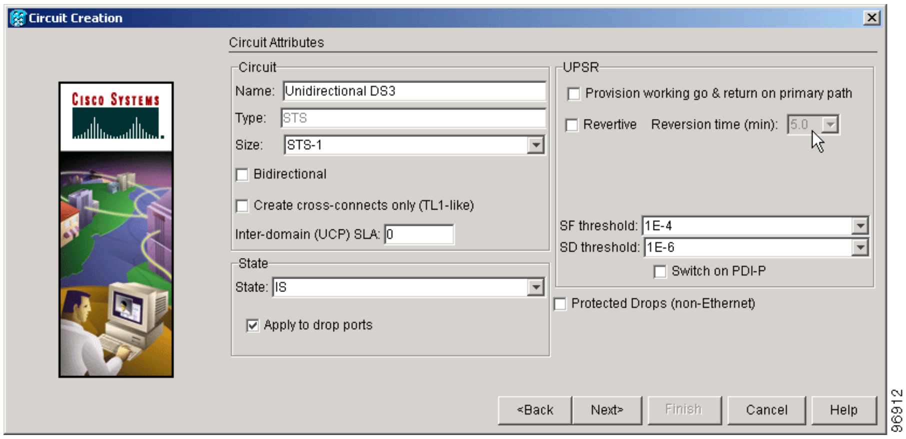
Step 7 Define the circuit attributes (Figure 8-8):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose **STS-1**. For circuits on the DS3i-N-12 card, choose **STS-3c**.
- Bidirectional—Uncheck for this circuit.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Figure 8-8 Setting Circuit Attributes for a Unidirectional DS-3 Circuit



Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A208 Provision a DS-3 Circuit Source and Destination" task on page 8-26.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-A96 Provision a DS-1 or DS-3 Circuit Route" task on page 8-16 for the DS-3 you are creating.

Step 17 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 18 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 19 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button while simultaneously pressing **Ctrl**, then dragging the icon to the new location.

Step 20 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 21 Click **Create**.

Step 22 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down menus. The card selected in Step b determines whether port, STS, or both appear. See Table 8-2 on page 8-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for option descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 12 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit State drop-down menu. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit State to the circuit source and destination drops.

g. Click **Finish**. The new drop appears in the Drops list.

Step 23 If you need to create additional drops for the circuit, repeat Steps 21 and 22 to create the additional drops.

Step 24 Click **Close**. The Circuits window appears.

Step 25 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 22 through 24, making sure all options are provisioned correctly.

Step 26 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-A133 Create an Automatically Routed VT Tunnel

Purpose	This procedure creates an automatically routed VT tunnel from source to destination nodes.This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through intermediary ONS 15454s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to create the VT tunnel. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

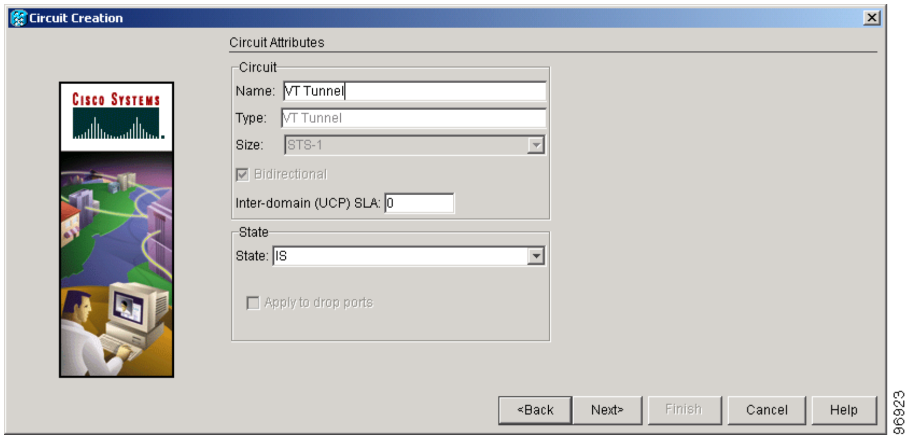
Step 5 In the Circuit Creation dialog box, choose **VT Tunnel** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-9):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- State—Choose a service state to apply to the VT tunnel:
  - IS—The VT tunnel is in service.
  - OOS—The VT tunnel is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The VT tunnel is in service when it receives a valid signal; until then, the tunnel is out of service.
  - OOS-MT—The VT tunnel is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the tunnel. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Unavailable for VT tunnels.
- Inter-domain (UCP) SLA—If the tunnel will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Figure 8-9 Setting Attributes for a VT Tunnel



Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down menu.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down menu.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.
- Review Route Before Creation—Check this check box to review and edit the VT tunnel route before the circuit is created.

Step 14 If you selected Using Required Nodes/Spans in Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a span on the VT tunnel map.

c. Click **Include** to include the node or span in the VT tunnel. Click **Exclude** to exclude the node or span from the VT tunnel. The order in which you choose included nodes and spans sets the VT tunnel sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the VT tunnel route. To change the tunnel routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the tunnel routing order. Click **Remove** to remove a node or span.

Step 15 If you selected Review Route Before Creation in Step 13:

a. Click **Next**.

b. Review the tunnel route. To add or delete a tunnel span, choose a node on the tunnel route. Blue arrows show the tunnel route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned tunnel does not reflect the routing and configuration you want, click **Back** to verify and change tunnel information.

Step 16 Click **Finish**. The Circuits window appears.

Step 17 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

NTP-A134 Create a Manually Routed VT Tunnel

Purpose	This procedure creates a manually routed VT tunnel from source to destination nodes. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through intermediary ONS 15454s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the VT tunnel. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

Step 5 In the Circuit Creation dialog box, choose **VT Tunnel** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-9 on page 8-34):

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- State—Choose a service state to apply to the VT tunnel:
  - IS—The VT tunnel is in service.
  - OOS—The VT tunnel is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The VT tunnel is in service when it receives a valid signal; until then, the circuit is out of service.

  - OOS-MT—The VT tunnel is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed. Use OOS-MT for testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Unavailable for VT tunnels.
- Inter-domain (UCP) SLA—If the tunnel will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down menu.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down menu.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 14 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the tunnel. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the tunnel.

Step 15 Complete the "DLP-A219 Provision a VT Tunnel Route" task on page 8-36 for the tunnel you are creating. The Circuits window appears.

Step 16 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

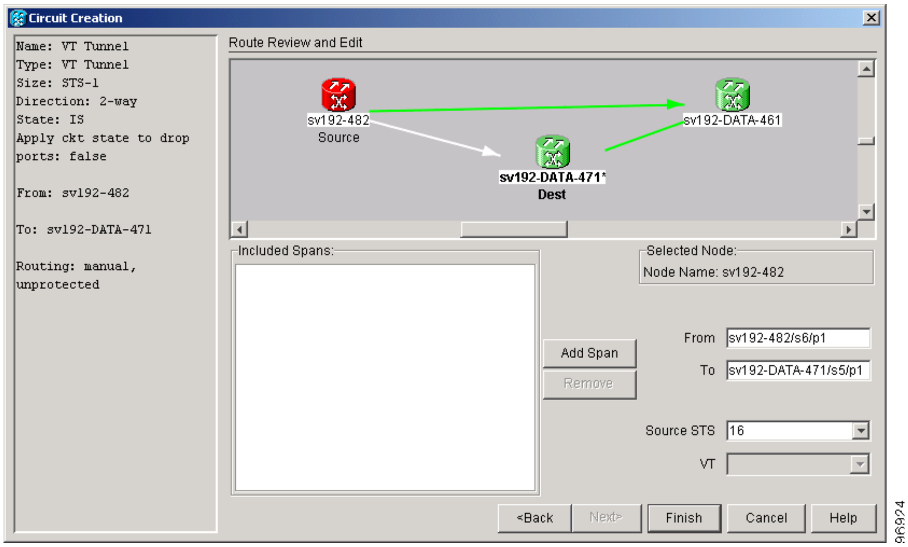
DLP-A219 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	The Circuit Creation wizard Route Review and Edit panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected. Arrows indicate the available spans for routing the tunnel from the source node.

Step 2 Click the arrow of the span you want the VT tunnel to travel. The arrow turns white. In the Selected Span area, the From and To fields show the slot and port that will carry the tunnel. The source STS appears. Figure 8-10 shows an example.

Figure 8-10 Manually Routing a VT Tunnel



Step 3 If you want to change the source STS, change it in the Source STS field; otherwise, continue with the next step.

Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 3 and 4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Return to your originating procedure (NTP).

NTP-A187 Create a VT Aggregation Point

Purpose	This procedure creates a VT aggregation point (VAP). VAPs allow multiple DS-1 (VT1.5) circuits to be aggregated on a single STS on an OC-N, EC-1, or DS3XM-6 card. VAPs allow multiple VT1.5 circuits to pass through cross-connect cards without utilizing resources on the cross-connect card VT matrix. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT aggregation points can be created for circuits on BLSR, 1+1, or unprotected nodes. They cannot be created for circuits on path protection nodes.

Note The maximum number of VAPs that you can create depends on the node protection topology and number of VT1.5 circuits that terminate on the node. Assuming no other VT1.5 circuits terminate at the node, the maximum number of VAPs that you can terminate at one node is 8 for 1+1 protection and 12 for BLSR protection.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the VT aggregation point. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

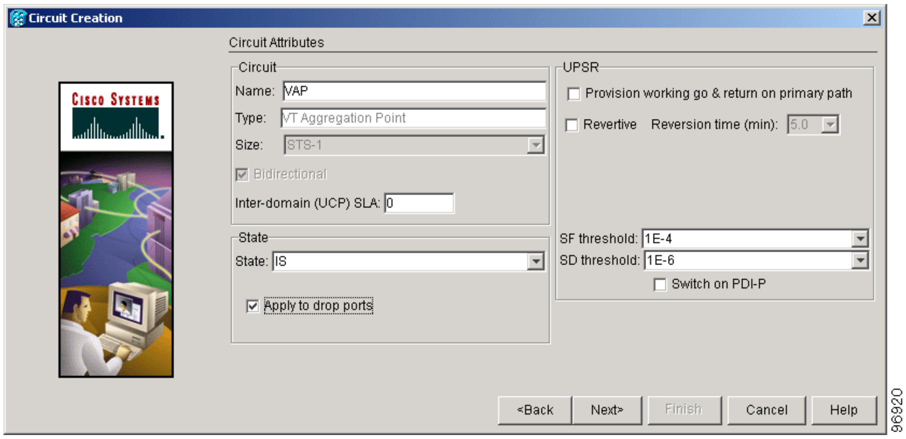
Step 5 In the Circuit Creation dialog box, choose **VT Aggregation Point** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes (Figure 8-11):

- Name—Assign a name to the VT aggregation point. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the VAP.
- Size—Unavailable for VAPs.
- Bidirectional—Unavailable for VAPs.
- State—Choose a service state to apply to the VAP:
  - IS—The VAP is in service.
  - OOS—The VAP is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The VAP is in service when it receives a valid signal; until then, the tunnel is out of service.
  - OOS-MT—The VAP is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the VAP. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Uncheck this box.
- Inter-domain (UCP) SLA—If the VAP will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Figure 8-11 Setting Attributes for a VT Aggregation Point



Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the source node, slot, port, and STS for the VAP. The VAP source is where the DS-1 (VT1.5) circuits will be aggregated into a single STS. The VAP destination is where the DS-1 circuits originate.

a. From the Node drop-down menu, choose the node where the VAP will originate.

b. From the Slot drop-down menu, choose the slot containing the OC-N, EC-1 or DS3XM-6 card where the VAP will originate.

c. Choose either the port or STS:

- If you choose an EC-1 or DS3XM-6 card, from the Port drop-down menu, choose the source port.
- If you choose an OC-N card, from the STS drop-down menu, choose the source STS.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the node where the VT circuits aggregated by the VAP will terminate from the Node drop-down menu.

Step 12 Click **Next**.

Step 13 In the Circuit Routing Preferences area, choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.
- Review Route Before Creation—Check this check box to review and edit the VT tunnel route before the circuit is created.

Step 14 If you selected Using Required Nodes/Spans in Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a span on the VAP map.

c. Click **Include** to include the node or span in the VAP. Click **Exclude** to exclude the node or span from the VAP. The sequence in which you choose the nodes and spans sets the VAP sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the VAP route. To change the tunnel routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the tunnel routing order. Click **Remove** to remove a node or span.

Step 15 If you selected Review Route Before Creation in Step 13:

a. Click **Next**.

b. Review the tunnel route. To add or delete a tunnel span, choose a node on the tunnel route. Blue arrows show the tunnel route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned tunnel does not reflect the routing and configuration you want, click **Back** to verify and change tunnel information.

Step 16 Click **Finish**. The Circuits window appears.

Step 17 Verify that the VAP you just created appears in the circuits list. VAPs are identified in the Type column.

Stop. You have completed this procedure.

NTP-A135 Test Electrical Circuits

Purpose	This procedures tests DS-1 and DS-3 circuits. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	A test set and all appropriate cables
Prerequisite Procedures	This procedure assumes you completed a facility loopback tests on the fibers and cables from the source and destination ONS 15454s to the DSX, and that you created a circuit using one of the following procedures: NTP-A181 Create an Automatically Routed DS-1 Circuit, page 8-6 NTP-A182 Create a Manually Routed DS-1 Circuit, page 8-13 NTP-A183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 8-18 NTP-A184 Create an Automatically Routed DS-3 Circuit, page 8-22 NTP-A185 Create a Manually Routed DS-3 Circuit, page 8-27 NTP-A186 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 8-29
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to test the electrical circuits. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Set the circuit and circuit ports to the maintenance state (OOS-MT). Take note of the original state because you will return the circuit to that state later.

a. Click the circuit you want to test, then choose **Circuits > Set Circuit State** from the Tools menu.

b. In the Set Circuit State dialog box, choose **OOS-MT** from the Target Circuit State drop-down menu.

c. Check the **Apply to drop ports** check box.

d. Click **Apply**.

Step 5 Set the source and destination DS-1 card line length:

a. In network view, double-click the source node.

b. Double-click the circuit source card and click the **Provisioning > Line** tabs.

c. From the circuit source port Line Length drop-down menu, choose the line length for the distance (in feet) between the DSX (if used) or circuit termination point and the source ONS 15454.

d. Click **Apply**.

e. From the View menu, choose **Go to Network View**.

f. Repeat Steps a through e for the destination port line length.

Step 6 Attach loopback cables to the circuit destination card:

a. Verify the integrity of the loopback cable by looping the test set transmit (Tx) connector to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.

b. Attach the loopback cable to the port you are testing. Connect the Tx connector to the Rx connector of the port.

Step 7 Attach loopback cables to the circuit source node:

a. Verify the integrity of loopback cable by looping the test set Tx connector to the test set Rx connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.

b. Attach the loopback cable to the port you are testing. Connect the test set to the circuit source port. Connect the Tx port of the test set to the circuit Rx port, and the test set Rx port to the circuit Tx port.

Step 8 Configure the test set for the ONS 15454 card that is the source of the circuit you are testing:

- DS-1—If you are testing an unmultiplexed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15454. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15454. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.
- DS3XM-6—If you are testing a DS-1 circuit on a DS3XM-6 card you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for a multiplexed DS3. After you choose multiplexed DS-3, choose the DS-1 to test on the multiplexed DS-3. For information about configuring your test set, consult your test set user guide.
- EC-1—If you are testing a DS-1 on an EC1 card, you must have a DSX-3 panel or a direct DS-3 interface to the ONS 15454. Set the test set for an STS-1. After you choose STS-1, choose the DS1 to test the STS-1. For information about configuring your test set, consult your test set user guide.

Step 9 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 2 through 8 to make sure the test set and cabling is configured correctly.

Step 10 Inject errors from the test set. Verify that the errors appear at the source and destination nodes.

Step 11 Clear the PM counts for the ports that you tested. See the "DLP-A349 Clear Selected PM Counts" task on page 10-8 for instructions.

Step 12 Return the circuit and circuit ports to the state they were in at the beginning of the test:

a. Click the circuit you want to test, then choose **Circuits > Set Circuit State** from the Tools menu.

b. In the Set Circuit State dialog box, choose **IS** (in service), **OOS** (out of service) or **OOS-AINS** (auto in service) from the Target Circuit State drop-down menu.

c. Check the **Apply to drop ports** check box.

d. Click **Apply**.

Step 13 Perform the protection switch test appropriate to the SONET topology:

- For path protections, complete the "DLP-A94 Path Protection Switching Test" task on page 6-40.
- For BLSRs complete the "DLP-A91 BLSR Switch Test" task on page 6-26.

Step 14 Perform a bit error rate test (BERT) for 12 hours or follow your site requirements for length of time. For information about configuring your test set for BERT, see your test set user guide.

Step 15 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A188 Create an Automatically Routed OC-N Circuit

Purpose	This procedure creates an automatically routed bidirectional or unidirectional OC-N circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c speeds. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **STS**.
- Number of Circuits—Type the number of OC-N circuits you want to create. The default is 1. If you are creating multiple circuits with the same source and destination, you can use auto-ranging to create the circuits automatically.

- Auto-ranged—This check box is automatically selected when you enter more than 1 in the Number of Circuits field. Leave this check box selected if you are creating multiple OC-N circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want CTC to create the circuits automatically.

Step 6 Click **Next**.

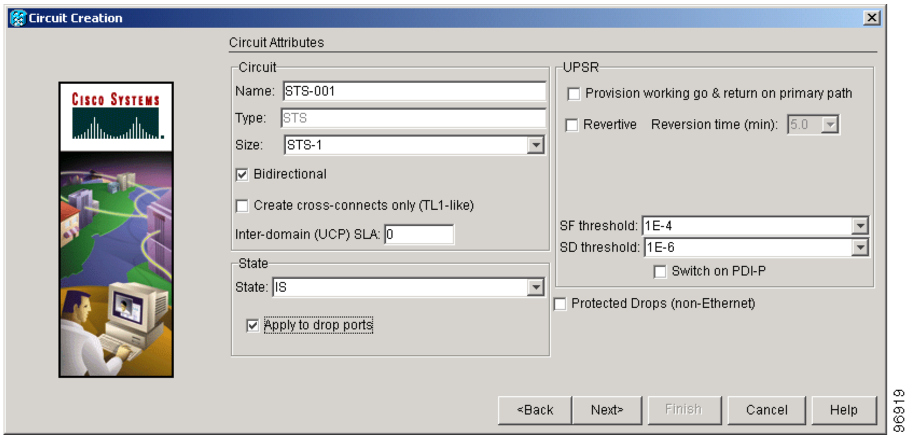
Step 7 Define the circuit attributes (Figure 8-12 on page 8-44):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the OC-N circuit size: STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

  Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protected drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Figure 8-12 Setting Circuit Attributes for an OC-N Circuit



Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

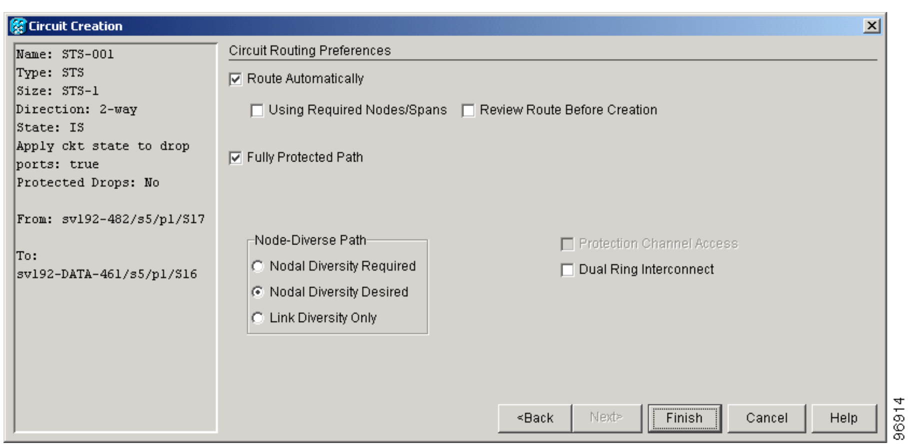
Step 9 Click **Next**.

Step 10 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 8-50 for the OC-N circuit you are creating.

Step 11 In the Circuit Routing Preferences area (Figure 8-13), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

Figure 8-13 Setting Circuit Routing Preferences for an OC-N Circuit



Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, click the **Dual Ring Interconnect** check box.

Step 15 If you selected Using Required Nodes/Spans in Step 11, complete the following substeps. If not, continue with Step 16:

a. Click **Next**.
b. In the Circuit Route Constraints area, click a node or span on the circuit map.
c. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.
d. Repeat Step c for each node or span you wish to include or exclude.
e. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you selected Review Route Before Creation in Step 11, complete the following substeps; otherwise, continue with Step 17:

a. Click **Next**.
b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.
c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A189 Create a Manually Routed OC-N Circuit" procedure on page 8-47 to assign the circuit route yourself.

Step 17 Click **Finish**. One of the following occurs, based on the circuit properties you provisioned in the Circuit Creation dialog box:

- If you entered more than 1 in the number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in Number of Circuits. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable on the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 18 In the Circuits window, verify that the circuit(s) you created appear in the circuits list.

Step 19 Complete the "NTP-A62 Test OC-N Circuits" procedure on page 8-54. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

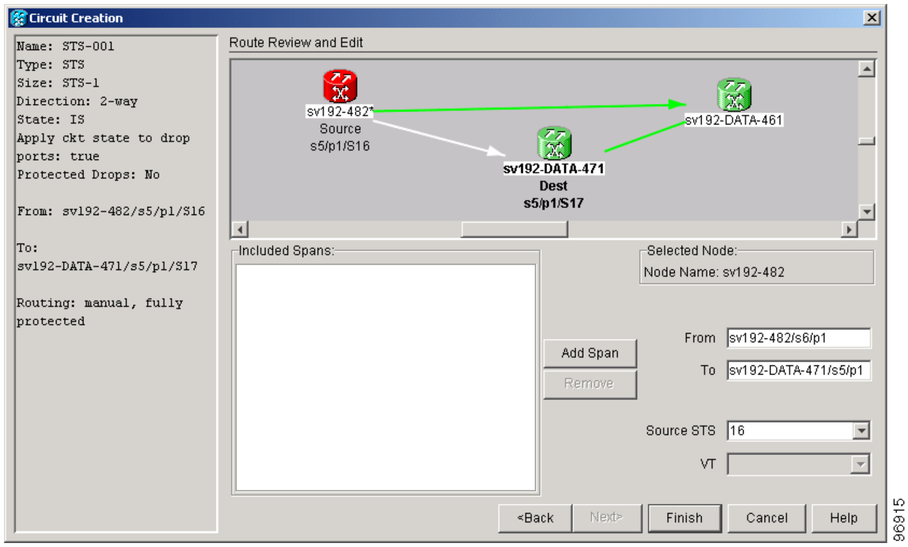
DLP-A98 Provision an OC-N Circuit Route

Purpose	This task provisions the circuit route for manually-routed OC-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 8-14 shows an example.

Figure 8-14 Manually Routing an OC-N Circuit



Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step 4.

> **Note** VT is gray for OC-N circuits.

Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protect Path is checked on the Circuit Routing Preferences panel, you must:

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination
- Add one span for all BLSR or 1+1 portions of route from the source to the destination

Step 6 Return to your originating procedure (NTP).

NTP-A189 Create a Manually Routed OC-N Circuit

Purpose	This procedure creates a manually routed, bidirectional or unidirectional, OC-N circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c speeds. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **STS**.
- Number of Circuits—Type the number of OC-N circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically routed circuits only. If you entered more than 1 in the Number of Circuits field, uncheck this box. (The box is unavailable if only one circuit is entered in Number of Circuits.)

Step 6 Click **Next**.

Step 7 Define circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the OC-N circuit size. Choices are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

  Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 8-50 for the OC-N circuit you are creating.

Step 11 In the Circuit Routing Preferences area (Figure 8-13 on page 8-44), uncheck **Route Automatically**.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually.

Step 16 Complete the "DLP-A98 Provision an OC-N Circuit Route" task on page 8-46.

Step 17 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path. If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears after the circuit is created so you can create the remaining circuits. Repeat Steps 5 through 17 for each additional circuit.

Step 18 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created appear in the window.

Step 19 Complete the "NTP-A62 Test OC-N Circuits" procedure on page 8-54.

Stop. You have completed this procedure.

DLP-A97 Provision an OC-N Circuit Source and Destination

Purpose	This task provisions an OC-N circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down menu, choose the node where the circuit will originate.

Step 2 From the Slot drop-down menu, choose the slot containing the OC-N card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the menu.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS from the Port and STS menus. The Port menu is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

> **Note** The STSs that appear depend on the card, circuit size, and protection scheme. For example, if you create an STS-3c circuit on an OC-12 card in a path protection, only four STSs are available. If you create an STS-3c circuit on an OC-12 card in a BLSR, two STSs are available because of the BLSR protection characteristics.

Step 4 If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu, choose the destination node.

Step 7 From the Slot drop-down menu, choose the slot containing the OC-N card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the menu.)

Step 8 Depending on the card selected in Step 2, choose the destination port and/or STS from the Port and STS submenus. The Port menu is available only if the card has multiple ports. The STSs that appear depend on the card, circuit size, and protection scheme.

Step 9 If you need to create a secondary destination, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

NTP-A190 Create a Unidirectional OC-N Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional OC-N circuit with multiple traffic drops (circuit destinations). This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 on the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.

Step 6 Click **Next**.

Step 7 Define circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size: STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c.
- Bidirectional—Uncheck this check box for this circuit.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15454 cards that are in 1:1, 1:N, or 1+1 protection. If you check this check box, CTC provides only protected cards as source and destination choices.

Step 8 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A97 Provision an OC-N Circuit Source and Destination" task on page 8-50 for the circuit you are creating.

Step 11 Uncheck **Route Automatically**. When Route Automatically is not selected, the Using Required Nodes/Spans and Review Route Before Circuit Creation check boxes are unavailable.

Step 12 To set the circuit path protection, complete one of the following:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 13. Fully protected paths might or might not have path protection path segments (with primary and alternate paths), and the path diversity options apply only to path protection path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** in the Warning dialog box, then continue with Step 15.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 13 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.

- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Note For manually routed circuits, CTC checks your manually provisioned path against the path diversity option you choose. If the path does not meet the path diversity requirement that is specified, CTC displays an error message.

Step 14 If you selected Fully Protected Path in Step 12 and the circuit will be routed on a path protection DRI, check the **Dual Ring Interconnect** check box.

Step 15 Click **Next**. In the Route Review and Edit area, node icons appear so you can route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-A98 Provision an OC-N Circuit Route" task on page 8-46.

Step 17 Click **Finish**. After completing the circuit, the Circuits window appears.

Step 18 In the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 19 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To see a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by pressing **Ctrl** while you drag and drop the icon to the new location.

Step 20 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 21 Click **Create**.

Step 22 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down menus. The choice in these menus depends on the card selected in Step b. See Table 8-2 on page 8-3 for a list of options.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

   - If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only. See Step 13 for option descriptions.
   - If the original circuit was not routed on a protected path, the Protection Channel Access option is available. See Step 12 for a description of the PCA option.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit State drop-down menu. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit State to the circuit source and destination drops.

g. Click **Finish**. The new drop appears in the Drops list.

Step 23 If you need to create additional drops on the circuit, repeat Steps 20 through 22.

Step 24 Click **Close**. The Circuits window appears.

Step 25 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 21 through 24, making sure all options are provisioned correctly.

Step 26 Complete the "NTP-A62 Test OC-N Circuits" procedure on page 8-54.

Stop. You have completed this procedure.

NTP-A62 Test OC-N Circuits

Purpose	This procedure tests an OC-N circuit. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	Test set capable of OC-N speeds, appropriate fibers, and attenuators
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution panel or the DSX and one of following circuit procedures: NTP-A188 Create an Automatically Routed OC-N Circuit, page 8-42 NTP-A189 Create a Manually Routed OC-N Circuit, page 8-47
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Set the circuit and circuit ports to OOS_MT:

- **a.** Click the circuit you want to test.
- **b.** From the Tools menu, choose **Circuits > Set Circuit State**.
- **c.** In the Set Circuit State dialog box, choose **OOS-MT** from the Target Circuit State drop-down menu.
- **d.** If unchecked, check the **Apply to drop ports** check box.
- **e.** Click **Apply**.

Step 5 Set up the patch cable at the destination node:

- **a.** Test the patch cable by connecting one end to the test set transmit (Tx) port and the other end to the test receive (Rx) port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.
- **b.** Install the loopback cable on the port you are testing. Connect the Tx connector to the Rx connector of the port being tested.

Step 6 Set up the loopback cable at the source node:

- **a.** Test the loopback cable by connecting one end to the test set Tx port and the other end to the test Rx port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.
- **b.** At the source node, attach the loopback cable to the port you are testing. Connect the test set to the circuit source port. Connect the Tx port of the test set to the circuit Rx port, and the test set Rx port to the circuit Tx port.

Step 7 Configure the test set for the source ONS 15454 card:

- OC-3 cards—You will test either an OC-3c or a multiplexed OC-3. If you are testing an OC-3c, configure the test set for an OC-3c. If you are testing a multiplexed OC-3, configure the test set for a multiplexed OC-3 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-12 cards—You will test either an OC-12c or a multiplexed OC-12. If you are testing an OC-12c, configure the test set for an OC-12c. If you are testing a multiplexed OC-12, configure the test set for a multiplexed OC-12 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-48 cards—You will test either an OC-48c or a multiplexed OC-48. If you are testing an OC-48c configure the test set for an OC-48c. If you are testing a multiplexed OC-48, configure the test set for a multiplexed OC-48 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-192 cards—You will test an OC-192c or a multiplexed OC-192. If you are testing an OC-192c configure the test set for an OC-192c. If you are testing a multiplexed OC-192, configure the test set for a multiplexed OC-192 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.

Step 8 Verify that the test set shows a clean signal. If a clean signal does not appear, repeat Steps 2 through 7 to make sure you have configured the test set and cabling correctly.

Step 9 Inject errors from the test set. Verify that the errors appear at the source and destination nodes.

Step 10 Clear the PM counts for the ports that you tested. See the "DLP-A349 Clear Selected PM Counts" task on page 10-8 for instructions.

Step 11 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, see the "DLP-A94 Path Protection Switching Test" task on page 6-40.
- For BLSRs see the "DLP-A91 BLSR Switch Test" task on page 6-26.

Step 12 Perform a bit error rate test (BERT) for 12 hours or follow your site requirements for length of time. For information about configuring your test set for the BERT, see your test set user guide.

Step 13 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Step 14 Change the circuit and circuit ports from OOS_MT to their previous service states:

a. Click the circuit you want to test, then from the Tools menu choose **Circuits > Set Circuit State**.

b. In the Set Circuit State dialog box, choose **IS** (in service), **OOS** (out of service), or **OOS-AINS** (auto inservice) from the Target Circuit State drop-down menu.

c. If unchecked, check the **Apply to drop ports** check box.

d. Click **Apply**.

Stop. You have completed this procedure.

NTP-A139 Create a Half Circuit on a BLSR or 1+1 Node

Purpose	This procedure creates a DS-1, DS-3, or OC-N circuit from a drop card to an OC-N trunk card on the same node in a BLSR or 1+1 topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node on the network where you will create the half circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—For DS-1 circuits, choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network. For DS-3 or OC-N circuits, choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Type the number of circuits you want to create. The default is 1.
- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For DS-3 or OC-N circuits, choose STS-1. For DS-1 circuits, VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Uncheck this box.

Step 8 Click **Next**.

Step 9 Complete the "DLP-A311 Provision a Half Circuit Source and Destination—BLSR and 1+1" task on page 8-58.

Step 10 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

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

Step 11 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 12 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-A311 Provision a Half Circuit Source and Destination—BLSR and 1+1

Purpose	This task provisions a half circuit source and destination for BLSR and 1+1 configurations. This task does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down menu, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down menu, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in Step 2.

Step 4 If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down menu.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu, choose the node chosen in Step 1.

Step 7 From the Slot drop-down menu, choose the OC-N card to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N STS circuit to an STS.

Step 8 Choose the destination STS or VT from the submenus that appear.

Step 9 Return to your originating procedure (NTP).

NTP-A140 Create a Half Circuit on a Path Protection Node

Purpose	This procedure creates a DS1, DS3, or OC-N circuit from a drop to an OC-N line card on the same path protection node. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

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

- Circuit Type—For DS1 circuits, choose **VT**. VT cross-connects will carry the DS-1 circuit across the ONS 15454 network. For DS-3 or OC-N circuits, choose **STS**. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- Number of Circuits—Type the number of circuits you want to create. The default is 1.
- Auto-ranged—Uncheck this check box; it is automatically selected if you enter more than 1 in the Number of Circuits field.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—For DS-1 circuits, VT1.5 is the default. You cannot change it. For DS-3 or OC-N circuits, choose STS-1.
- Bidirectional—Leave checked for this circuit (default).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

  Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave this box unchecked.

Step 8 Set the path protection path selectors. See the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 9 Click **Next**.

Step 10 Complete the "DLP-A312 Provision a Half Circuit Source and Destination—Path Protection" task on page 8-60.

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

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in Number of Circuits. If auto-ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click Finish to continue auto-ranging. After completing the circuit(s), the Circuits window appears.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears so you can create the remaining circuits. Repeat Steps 5 through 11 for each additional circuit. After completing the circuit(s), the Circuits window appears.

Step 12 In the Circuits window, verify that the new circuits appear in the circuits list.

Step 13 Complete the "NTP-A135 Test Electrical Circuits" procedure on page 8-40. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-A312 Provision a Half Circuit Source and Destination—Path Protection

Purpose	This task provisions a half circuit source and destination for a path protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	The Circuit Creation wizard Circuit Source panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu, choose the node that will contain the half circuit.

Step 2 From the Slot drop-down menu, choose the slot containing the card where the circuit will originate.

Step 3 From the Port drop-down menu, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in Step 2.

Step 4 If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down menu.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu, choose the node selected in Step 1.

Step 7 From the Slot drop-down menu, choose the OC-N card to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N STS circuit to an STS.

Step 8 Choose the destination STS or VT from the drop-down menus that appear.

Step 9 Click **Use Secondary Destination** and repeat Steps 1 through 8.

Step 10 Return to your originating procedure (NTP).

NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode)

Purpose	This procedure creates a multicard or single-card EtherSwitch circuit. It does not apply to E-Series cards in port-mapped mode. To create a port-mapped mode circuit, see NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 8-68.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the EtherSwitch circuit. If you are already logged in, continue with Step 2.

Step 2 If a high number of VLANs is already used by the network, complete the "DLP-A99 Determine Available VLANs" task on page 8-64 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 If enough VLANs are not available, complete the "DLP-A335 Delete VLANS" task on page 8-65 to free space.

Step 4 Verify that the circuit source and destination Ethernet cards are provisioned for the mode of the circuit you will create, either multicard or single-card. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 5 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 6 From the View menu, choose **Go to Network View**.

Step 7 Click the **Circuits** tab, then click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid circuit sizes for an Ethernet multicard circuit are STS-1, STS-3c, and STS6c. Valid circuit sizes for an Ethernet single-card circuit are STS-1, STS-3c, STS6c, and STS12c.
- Bidirectional—Leave the default unchanged (checked).
- State—Choose **IS** (in service). Ethergroup circuits are stateless and always in service.
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.
- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Caution Layer 1 SONET protection does not extend to multicard EtherSwitch circuits on path protection.

Caution A TCC2 card reset disrupts single-card and multicard Etherswitch circuits for 45 seconds to two minutes. During this time a spanning tree topology is created by the newly activated TCC2 card.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down menu, choose one of the EtherSwitch circuit endpoint nodes. (Either end node can be the EtherSwitch circuit source.)

b. From the Slot drop-down menu, choose one of the following:
   - If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
   - If you are building a single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down menu, choose the second EtherSwitch circuit endpoint node.

b. From the Slot drop-down menu, choose one of the following:
   - If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
   - If you are building a single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 16 Click **Next**.

Step 17 In the Circuit VLAN Selection area, click **New VLAN**. If the desired VLAN already exists, continue with Step 20.

Tip You can also add VLANs in network view by choosing Tools > Manage VLANs. In the All VLANs dialog box, click the Create button to open the Define New VLAN dialog box.

Step 18 In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology ID—Choose the topology ID from the drop-down menu.

Step 19 Click **OK**.

Step 20 In the Circuit VLAN Selection area, highlight the VLAN name and click the arrow button (>>) to move the available VLAN(s) to the Circuit VLANs column.

Step 21 If you are building a single-card EtherSwitch circuit and want to disable spanning tree protection on this circuit, uncheck the **Enable Spanning Tree** check box and click **OK** in the Disabling Spanning Tree dialog box. The Enable Spanning Tree box remains checked or unchecked for the creation of the next single-card, point-to-point Ethernet circuit.

Caution Disabling spanning-tree protection increases the likelihood of logic loops on an Ethernet network.

Caution Turning off spanning tree on a circuit-by-circuit basis means that the ONS 15454 is no longer protecting the Ethernet circuit and that the circuit must be protected by another mechanism in the Ethernet network.

Caution Multiple circuits with spanning tree protection enabled incur blocking if the circuits traverse the same E-Series card and use the same VLAN.

Note Spanning-tree rules prevent users from creating new circuits or modifying existing circuits if the circuits do not meet certain VLAN assignment constraints. If the VLAN set of the new circuit overlaps existing circuits, the same spanning-tree instance is used for all circuits. If the VLAN set of the new circuit overlaps with VLAN sets of existing circuits with different spanning-tree instances, the VLAN assignment fails. Cisco recommends that you plan VLAN assignments so that circuits with larger VLAN sets and a higher chance of overlap are added first. This means that if a circuit with an overlapping VLAN set is added, it collapses into the same spanning tree. To view circuits mapped to a spanning tree and their VLAN assignments, see the "DLP-A430 View Spanning Tree Information" task on page 11-11.

Note You can disable or enable spanning tree protection on a circuit-by-circuit basis only for single-card, point-to-point Ethernet circuits. Other E-Series Ethernet configurations disable or enable spanning tree on a port-by-port basis.

Step 22 Click **Next**.

Step 23 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 nodes

Step 24 If the information is not correct, click the **Back** button and repeat Steps 8 through 23 with the correct information. If the information is correct, check **Route Automatically**.

Step 25 Click **Finish**.

Step 26 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67.

Stop. You have completed this procedure.

DLP-A99 Determine Available VLANs

Purpose	This task verifies that the network has the capacity to support the additional new VLANs required for the creation E-Series circuits. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In any CTC view, click the **Circuits** tab.

Step 2 Click any existing Ethernet circuit.

Step 3 Click **Edit**, then click the **VLANs** tab.

The Edit Circuit dialog shows the number of VLANs used by circuits and the total number of VLANs available for use.

Step 4 Determine that number of available VLANs listed is sufficient for the number of E-Series Ethernet circuits that you will create.

Caution Multiple E-Series Ethernet circuits with spanning tree enabled block each other if the circuits traverse the same E-Series Ethernet card and use the same VLAN.

Step 5 Return to the originating procedure (NTP).

DLP-A335 Delete VLANS

Purpose	This task removes VLANs from a domain.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 From the Tools menu, choose **Manage VLANS**.

Step 3 In the All VLANs dialog box, click the VLAN that you want to remove.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-A246 Provision E-Series Ethernet Card Mode

Purpose	This task provisions an E-Series Ethernet card for multicard EtherSwitch Group, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution You cannot change the mode while the Ethernet card is carrying circuits. If you want change the card mode, delete any circuits that it carries first. See the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19.

Step 1 In the network view, double-click the node containing the E-Series Ethernet card you want to provision, then double-click the Ethernet card.

Step 2 Click the **Provisioning > Ether Card** tabs.

Step 3 In the Card Mode area, choose one of the following:

- For multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group**.
- For single-card EtherSwitch circuits, choose **Single-card EtherSwitch**.
- For port-mapped circuits, choose **Port-mapped**.

Step 4 Click **Apply**.

Step 5 If you are using multicard EtherSwitch circuits, repeat Steps 2 through 4 for all other Ethernet cards in the node that will carry the multicard EtherSwitch circuits.

Step 6 Repeat Steps 1 through 5 for other nodes as necessary.

Step 7 Return to your originating procedure (NTP).

DLP-A220 Provision E-Series Ethernet Ports

Purpose	This task enables the E100T-12, E100T-G, E1000-2, and E1000-2-G ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

Step 1 In node view, double-click the Ethernet card that you want to provision.

Step 2 Click the **Provisioning** > **Ether Port** tabs.

Step 3 For each Ethernet port, provision the following parameters:

- Port Name—If you want to label the port, type a port name.
- Mode—Choose the appropriate mode for the Ethernet port:
  - Valid choices for the E100T-12/E100T-G card are Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
  - Valid choices for the E1000-2/E1000-2-G card are 1000 Full or Auto.

Note Both 1000 Full and Auto mode set the E1000-2 port to the 1000 Mbps and Full duplex operating mode; however, flow control is disabled when 1000 Full is selected. Choosing Auto mode enables the E1000-2 card to autonegotiate flow control. Flow control is a mechanism that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. The E1000-2 port handshakes with the connected network device to determine if that device supports flow control.

- Enabled—Check this check box to activate the corresponding Ethernet port.
- Priority—Choose a queuing priority for the port. Options range from 0 (Low) to 7 (High). Priority queuing (IEEE 802.1Q) reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. Refer to the priority queuing information in the *Cisco ONS 15454 Reference Manual*. This parameter does not apply to an E-Series card in port-mapped mode.
- Stp Enabled—Check this check box to enable the Spanning Tree Protocol (STP) on the port. This parameter does not apply to an E-Series card in port-mapped mode. Refer to the spanning tree information in the *Cisco ONS 15454 Reference Manual*.

Step 4 Click **Apply**.

Step 5 Repeat Steps 1 through 4 for all other cards in the VLAN, or if the E-Series card is in port-mapped mode, repeat Steps 1 through 4 for the other card in a point-to-point circuit.

Step 6 Your Ethernet ports are provisioned and ready to be configured for VLAN membership. See the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67 for instructions.

Step 7 Return to your originating procedure (NTP).

DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership

Purpose	This task provisions E-Series card ports for VLAN membership. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the E-Series card graphic to open the card.

Step 2 Click the **Provisioning** > **Ether VLAN** tabs.

Step 3 To put a port in a VLAN:

a. Click the port and choose either **Tagged** or **Untag**.

b. If a port is a member of only one VLAN, choose **Untag** from the Port column in the VLAN's row. Choose **--** for all the other VLAN rows in that Port column.

Note The VLAN with Untag selected can connect to the port, but other VLANs cannot access that port.

c. Choose **Tagged** at all VLAN rows that need to be trunked. Choose **Untag** at VLAN rows that do not need to be trunked, for example, the default VLAN.

Note Each Ethernet port must be attached to at least one untagged VLAN. A trunk port connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (IEEE 802.1Q) enabled for all the VLANs that connect to that external device.

Step 4 After each port is in the appropriate VLAN, click **Apply**. Table 8-4 lists VLAN settings.

Table 8-4 VLAN Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.

Table 8-4 VLAN Settings (continued)

Setting	Description
Untag	The ONS 15454 tags ingress frames and strips tags from egress frames.
Tagged	The ONS 15454 processes ingress frames according to the VLAN ID; egress frames do not have their tags removed.

Note If Tagged is chosen, the attached external Ethernet devices must recognize IEEE 802.1Q VLANs.

Note Both ports on an E1000-2/E1000-2-G card cannot be members of the same VLAN.

Step 5 Return to your originating procedure (NTP).

NTP-A192 Create a Circuit for an E-Series Card in Port-Mapped Mode

Purpose	This procedure creates an E-Series point-to-point SONET circuit with an E-Series card in port-mapped mode.
Tools/Equipment	An E-Series Ethernet card must be installed at each end of the circuit and configured in port-mapped mode.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 4.

Step 2 Provision the Ethernet cards that will carry the circuit for port-mapped mode. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 3 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab and click **Create**.

Step 6 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid circuit sizes for an E-Series circuit are STS-1, STS-3c, STS6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to E-Series Ethernet card ports. CTC applies the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box shows the ports where the circuit state could not be applied. If the box is unchecked, CTC does not change the state of the source and destination ports.

  Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Auto-ranged—Unavailable.
- Protected Drops—Leave the default unchanged (unchecked).

Step 9 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 10 Click **Next**.

Step 11 Provision the circuit source:

a. From the Node drop-down menu, choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down menu, choose the slot containing the E-Series card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down menu, choose a port.

Step 12 Click **Next**.

Step 13 Provision the circuit destination:

a. From the Node drop-down menu, choose the circuit destination node.

b. From the Slot drop-down menu, choose the slot containing the E-Series card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down menu, choose a port.

Step 14 Click **Next**.

Step 15 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 nodes

Step 16 If the information is not correct, click the **Back** button and repeat Steps 6 through 15 with the correct information. If the information is correct, check **Route Automatically**.

Step 17 Click **Finish**.

Step 18 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 8-81.

Stop. You have completed this procedure.

NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit

Purpose	This procedure creates a shared packet ring Ethernet circuit. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at both Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If a high number of VLANs is already used by the network, complete the "DLP-A99 Determine Available VLANs" task on page 8-64 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Verify that the Ethernet cards that will carry the circuit are provisioned for the Multicard EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 4 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 5 From the View menu, choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 8 Click **Next**.

Step 9 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid shared packet ring circuit sizes are STS-1, STS-3c, and STS6c.
- Bidirectional—Leave the default unchanged (checked).
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series ports.
- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 10 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Caution Layer 1 SONET protection does not extend to multicard EtherSwitch circuits on path protection.

Step 11 Click **Next**.

Step 12 Provision the circuit source:

a. From the Node drop-down menu, choose one of the shared packet ring circuit endpoint nodes. (Either end node can be the shared packet ring circuit source.)
b. From the Slot drop-down menu, choose **Ethergroup**.

Step 13 Click **Next**.

Step 14 Provision the circuit destination:

a. From the Node drop-down menu, choose the second shared packet ring circuit endpoint node.
b. From the Slot drop-down menu, choose **Ethergroup**.

Step 15 Click **Next**.

Step 16 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 17. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.
b. In the Define New VLAN dialog box, complete the following:
    - VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology ID—Choose the topology ID from the drop-down menu.

c. Click **OK**.

> **Tip** You can also add VLANs in network view by choosing Tools > Manage VLANs. In the All VLANs dialog box, click the Create button to open the Define New VLAN dialog box.

Step 17 In the Available VLANs column, click the VLAN you want to use and click the arrow button (>>) to move the VLAN to the Circuit VLANs column.

> **Note** Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 18 Click **Next**.

Step 19 In the Circuit Routing Preferences area, uncheck the **Route Automatically** check box and click **Next**.

Step 20 In the Route Review and Edit area, click the source node, then click a span (green arrow) leading away from the source node.

The span turns white.

Step 21 Click **Add Span**.

The span turns blue. CTC adds the span to the Included Spans list.

Step 22 Click the node at the end of the blue span.

Step 23 Click the green span joining the node selected in Step 22.

The span turns white.

Step 24 Click **Add Span**.

The span turns blue.

Step 25 Repeat Steps 21 through 24 for every node in the ring.

Step 26 In the Route Review and Edit area, verify that the new circuit is correctly configured. If the circuit information is not correct, click the **Back** button and repeat Steps 7 through 25 with the correct information.

> **Note** If the circuit is incorrect, you can also click **Finish**, delete the completed circuit, and begin the procedure again.

Step 27 Click **Finish**.

Step 28 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66 for each node that carries the circuit.

Step 29 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67 for each node that carries the circuit.

Step 30 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 8-81.

Stop. You have completed this procedure.

NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration

Purpose	This procedure creates a hub-and-spoke Ethernet configuration, which is made up of multiple circuits that share a common endpoint. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at all Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the hub node (the common endpoint). If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A99 Determine Available VLANs" task on page 8-64 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Display the node view.

Step 4 Verify that the Ethernet card that will carry the hub-and-spoke circuit is provisioned for Single-card EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 5 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 6 Log into a spoke endpoint node and repeat Steps 3 through 5 for the destination Ethernet card. You only need to verify that the hub node is provisioned for single-card EtherSwitch once.

Step 7 Click the **Circuits** tab and click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size.
- Bidirectional—Leave the default unchanged (checked).
- State—The circuit is in service (default).

- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series ports.
- Create cross-connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down menu, choose the hub node.

b. From the Slot drop-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down menu, choose an EtherSwitch circuit endpoint node.

b. From the Slot drop-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 16 Click **Next**.

Step 17 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 19. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology ID—Choose the topology ID from the drop-down menu.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing Tools > Manage VLANs. In the All VLANs dialog box, click the Create button to open the Define New VLAN dialog box.

Step 18 In the Available VLANs column, click the VLAN you want to use and click the arrow button (**>>**) to move the VLAN to the Circuit VLANs column.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 19 Click **Next**.

Step 20 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:

- Circuit name

- Circuit type
- Circuit size
- VLAN names
- ONS 15454 nodes

Step 21 If the information is not correct, click the **Back** button and repeat Steps 8 through 20 with the correct information. If the information is correct, check **Route Automatically**.

Step 22 Click **Finish**.

Step 23 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 24 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67.

Step 25 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 8-81.

Step 26 To create additional circuits (spokes), repeat Steps 2 through 25.

Stop. You have completed this procedure.

NTP-A144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect

Purpose	This procedure manually creates a single-card EtherSwitch cross-connect between E-Series Ethernet cards and OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

Step 3 If a high number of VLANs is already used by the network, complete the "DLP-A99 Determine Available VLANs" task on page 8-64 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 4 In the node view, double-click the Ethernet card that will carry the cross-connect.

Step 5 Verify that the Ethernet cards that will carry the circuit are provisioned for single-card EtherSwitch. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 6 From the View menu, choose **Go to Network View**.

Step 7 Click the **Circuits** tab and click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).

Step 9 Click **Next**.

Step 10 Define the circuit attributes:

- Name—Assign a name to the cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the cross-connect.
- Size—Choose the cross-connect size. For single-card EtherSwitch, the available sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Create cross-connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 11 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 12 Click **Next**.

Step 13 Provision the circuit source:

a. From the Node drop-down menu, choose the cross-connect source node.

b. From the Slot drop-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch in Step 5.

Step 14 Click **Next**.

Step 15 Provision the circuit destination:

a. From the Node drop-down menu, choose the cross-connect circuit source node selected in Step 13. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot drop-down menu, choose the OC-N card that is connected to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and/or STS from the Port and STS drop-down menus.

Step 16 Click **Next**.

Step 17 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 18. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:

   - VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
- Topology ID—Choose the topology ID from the drop-down menu.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing Tools > Manage VLANs. In the All VLANs dialog box, click the Create button to open the Define New VLAN dialog box.

Step 18 Click the VLAN you want to use on the Available VLANs column, then click the arrow **>>** button to move the VLAN to the Circuit VLANs column.

Step 19 Click **Next**.

Step 20 In the left pane of the Circuit Routing Preferences panel, confirm that the following information about the single-card EtherSwitch manual cross-connect is correct (in this task, "circuit" refers to the Ethernet cross-connect):

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15454 nodes

Step 21 If the information is not correct, click the **Back** button and repeat Steps 8 through 20 with the correct information. If the information is correct, check **Route Automatically**.

Step 22 Click **Finish**.

Step 23 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 24 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67.

Stop. You have completed this procedure.

NTP-A145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect

Purpose	This procedure manually creates multicard EtherSwitch cross-connects between E-Series Ethernet cards and an OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A99 Determine Available VLANs" task on page 8-64 to verify that sufficient VLAN capacity is available. (You will create a VLAN during each circuit creation task.)

Step 3 Verify that the Ethernet card that will carry the circuit is provisioned for Multicard EtherSwitch Group. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 4 Provision and enable the Ethernet ports. See "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 5 From the View menu, choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 8 Click **Next**.

Step 9 Define the circuit attributes:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Size—Choose the size of the circuit that will be carried by the cross-connect. For multicard EtherSwitch circuits, the available sizes are STS-1, STS-3c, and STS-6c.
- Bidirectional—Leave checked (default).
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Create cross-connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 10 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 11 Click **Next**.

Step 12 Provision the cross-connect source:

a. From the Node drop-down menu, choose the cross-connect source node.

b. From the Slot drop-down menu, choose **Ethergroup**.

Step 13 Click **Next**.

Step 14 From the Node drop-down menu in the Destination area, choose the circuit source node selected in Step 12. For Ethernet cross-connects, the source and destination nodes are the same.

The Slot field is provisioned automatically for Ethergroup.

Step 15 Click **Next**.

Step 16 Review the VLANs listed in the Available VLANs list. If the VLAN you want to use appears, continue with Step 18. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. In the Define New VLAN dialog box, complete the following:
   - VLAN Name—Assign an easily identifiable name to your VLAN.
   - VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
   - Topology ID—Choose the topology ID from the drop-down menu.

c. Click **OK**.

Tip You can also add VLANs in network view by choosing Tools > Manage VLANs. In the All VLANs dialog box, click the Create button to open the Define New VLAN dialog box.

Step 17 In the Available VLANs column, click the VLAN you want to use and click the arrow button (>>) to move the VLAN to the Circuit VLANs column.

Step 18 Click **Next**.

Step 19 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:
- Circuit name
- Circuit type
- Circuit size
- VLANs
- ONS 15454 nodes

Step 20 If the information is not correct, click the **Back** button and repeat Steps 7 through 19 with the correct information. If the information is correct, check **Route Automatically**.

Step 21 Click **Finish**.

Step 22 Complete the "DLP-A220 Provision E-Series Ethernet Ports" task on page 8-66.

Step 23 Complete the "DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 8-67.

Step 24 From the View menu, choose **Go to Home View**.

Step 25 Click the **Circuits** tab.

Step 26 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box appears.

Step 27 In the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 28 Click **Create**.

Step 29 In the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the OC-N card that links the ONS 15454 to the non-ONS 15454 equipment.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down menus.

d. The routing preferences for the new drop match those of the original circuit. However, if the following options are available, you can modify them:

- If the original circuit was routed on a protected path protection path, you can change the nodal diversity options: Nodal Diversity Required, Nodal Diversity Desired, or Link Diversity Only.
- If the original circuit was not routed on a protected path, the Protection Channel Access option is available.

e. If you want to change the circuit state, choose the circuit state from the Target Circuit State drop-down menu. The state chosen applies to the entire circuit.

f. Check **Apply to drop ports** if you want to apply the state chosen in the Target Circuit State to the circuit source and destination drops.

g. Click **Finish**. The new drop appears in the Drops list.

Step 30 Confirm the circuit information that appears in the Edit Circuit dialog box and click **Close**.

Step 31 Repeat Steps 2 through 30 at the second Ethernet manual cross-connect endpoint.

The first and second Ethernet manual cross-connect endpoints will be bridged by the OC-N STS cross-connect circuit.

Note The appropriate STS circuit must exist in the non-ONS equipment to connect the two Ethernet manual cross-connect endpoints.

Caution If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits might have a circuit-size mismatch. For example, a circuit size of STS-3c was configured on the first ONS 15454 and circuit size of STS-12c was configured on the second ONS 15454. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if the alarm persists.

Step 32 Complete the "NTP-A146 Test E-Series Circuits" procedure on page 8-81.

Stop. You have completed this procedure.

NTP-A146 Test E-Series Circuits

Purpose	This procedure tests circuits created on E-Series Ethernet cards provisioned for multicard EtherSwitch, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution panel or the DSX, and one of the following: NTP-A191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 8-61 NTP-A142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 8-70 NTP-A143 Create an E-Series Hub-and-Spoke Ethernet Configuration, page 8-73
Required/As Needed	As needed
Onsite/Remote	Onsite
Security	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the ONS 15454 source Ethernet node.

Step 2 On the shelf graphic, double-click the circuit source card.

Step 3 Click the **Provisioning > Ether Port** tabs.

Step 4 Verify the following settings:

- Mode—Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
- Enabled—Checked.
- Priority—Set to the priority level indicated by the circuit or site plan. Priority does not apply to E-Series cards in port-mapped mode.
- Stp State—Checked if Spanning Tree Protocol is enabled for the circuit. Stp does not apply to E-Series cards in port-mapped mode.

Step 5 Click the **Ether VLAN** tab. If the E-Series cards is not in port-mapped mode, verify that the source port is on the same VLAN as the destination port.

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test set to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

> **Note** At this point, you are not able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, see the "DLP-A94 Path Protection Switching Test" task on page 6-40.
- For BLSRs see the "DLP-A91 BLSR Switch Test" task on page 6-26.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 After the Ethernet test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A147 Create a G-Series STS Circuit

Purpose	This procedure creates a G-Series circuit.
Tools/Equipment	A G-Series Ethernet card must be installed at each end of the circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab and click **Create**.

Step 4 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 5 Click **Next**.

Step 6 Define the circuit attributes:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose the circuit size. Valid circuit sizes for a G-Series circuit are STS-1, STS-3c, STS6c, STS-9c, STS-12c, STS-24c, and STS-48c.

Note Restrictions apply to provisioning multiple circuits on a G-Series card when one of the circuit sizes provisioned is STS-24c. Refer to the *Cisco ONS 15454 Reference Manual* for complete information.

- Bidirectional—Leave the default unchanged (checked).

- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Leave this box at the default (unchecked).

  Note Loss of signal alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Auto-ranged—Unavailable.
- Protected Drops—Leave the default unchanged (unchecked).

Step 7 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Note For circuits routed on path protection, check **Switch on PDI-P** if you desire to override the G-Series Ethernet Link Integrity feature. Switch on PDI-P configures the card to switch traffic when an STS payload defect indicator (PDI-P) is received. Under Ethernet Link Integrity, the PDI-P indication normally triggers a bidirectional failure. Overriding the Ethernet Link Integrity feature might be desired for applications utilizing dual Gigabit Ethernet feeds from a customer's location or drop and continue paths.

Step 8 Click **Next**.

Step 9 Provision the circuit source:

a. From the Node drop-down menu, choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down menu, choose the slot containing the G-Series card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down menu, choose a port.

Step 10 Click **Next**.

Step 11 Provision the circuit destination:

a. From the Node drop-down menu, choose the circuit destination node.

b. From the Slot drop-down menu, choose the slot containing the G-Series card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down menu, choose a port.

Step 12 Click **Next**.

Step 13 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 nodes

Step 14 If the information is not correct, click the **Back** button and repeat Steps 4 through 13 with the correct information. If the information is correct, check **Route Automatically**.

Step 15 Click **Finish**.

Note To change the capacity of a G-Series circuit, you must delete the original circuit and reprovision a new larger circuit.

Step 16 Complete the "NTP-A149 Test G-Series Circuits" procedure on page 8-91.

Stop. You have completed this procedure.

NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode

Purpose	This procedure creates a manual cross-connect between a G-Series Ethernet card or an E-Series Ethernet card in port-mapped mode and an OC-N card connected to non-ONS equipment.
Tools/Equipment	A G-Series or E-Series card must be installed at the circuit source node.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the cross-connect. If you are already logged in, continue with Step 2.

Step 2 If you are provisioning an E-Series card, verify that the Ethernet card that will carry the circuit is provisioned for port-mapped mode. See the "DLP-A246 Provision E-Series Ethernet Card Mode" task on page 8-65.

Step 3 If you are provisioning a G-Series card, complete the "DLP-A222 Provision G-Series Ethernet Ports" task on page 8-86.

Step 4 If you want to change the default flow control settings, complete the "DLP-A421 Provision G-Series Flow Control Watermarks" task on page 8-87.

Step 5 Click the **Circuits** tab and click **Create**.

Step 6 In the Create Circuits dialog box, complete the following fields:

- Circuit Type—Choose **STS**.
- Number of Circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.

Step 7 Click **Next**.

Step 8 Define the circuit attributes:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Size—Choose the size of the circuit that will be carried by the cross-connect. Valid sizes for a G-Series circuit are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c. For an E-Series card in port-mapped mode, valid sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- State—The circuit is in service (default).
- Apply to drop ports—Uncheck this box.
- Create cross-connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 9 If the circuit will be routed on a path protection, complete the "DLP-A218 Provision Path Protection Selectors During Circuit Creation" task on page 8-11.

Step 10 Click **Next**.

Step 11 Provision the circuit source:

a. From the Node drop-down menu, choose the circuit source node.

b. From the Slot drop-down menu, choose the Ethernet card that will be the cross-connect source.

c. From the Port drop-down menu, choose the cross-connect source port.

Step 12 Click **Next**.

Step 13 Provision the circuit destination:

a. From the Node drop-down menu, choose the cross-connect source node selected in Step 11. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot drop-down menu, choose the OC-N card that connects to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and STS from the Port and STS drop-down menus.

Step 14 Click **Next**.

Step 15 In the left pane of the Circuit Routing Preferences panel, confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size

- ONS 15454 nodes

Step 16 If the information is not correct, click the **Back** button and repeat Steps 5 through 15 with the correct information. If the information is correct, check **Route Automatically**.

Step 17 Click **Finish**.

Stop. You have completed this procedure.

DLP-A222 Provision G-Series Ethernet Ports

Purpose	This task provisions G-Series Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the G-Series card graphic to open the card.

Step 2 Click the **Provisioning** > **Port** tabs.

Step 3 For each G-Series port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- State—Choose **IS** to put the port in service.
- Flow Control Neg—Check this check box to enable flow control negotiation on the port (default). If you do not want to enable flow control, uncheck the box.

  Note To activate flow control, the Ethernet device attached to the G-Series card must be set to autonegotiation. If flow control is enabled but the negotiation status indicates no flow control, check the autonegotiation settings on the attached Ethernet device.

- Max Size—To permit the acceptance of jumbo size Ethernet frames, choose **Jumbo** (default). If you do not want to permit jumbo size Ethernet frames, choose **1548**.

Note The maximum frame size of 1548 bytes enables the port to accept valid Ethernet frames that use protocols, such as ISL. ISL adds 30 bytes of overhead and might cause the frame size to exceed the traditional 1518 byte maximum.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the G-Series card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-A421 Provision G-Series Flow Control Watermarks

Purpose	This task provisions the buffer memory levels for flow control on G-Series Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the G-Series card graphic to open the card.

Step 2 Click the **Provisioning** > **Port** tabs.

Step 3 In the Water Marks column, click the cell in the row for the appropriate port.

Step 4 To provision the Low Latency flow control watermark:

a. Choose **Low Latency** from the drop-down menu.

The Flow Ctrl Lo and Flow Ctrl Hi values change.

b. Click **Apply**.

Step 5 To provision a Custom flow control watermark:

a. Choose **Custom** from the drop-down menu.

b. In the Flow Ctrl Lo column, click the cell in the row for the appropriate port.

c. Enter a value in the cell. The Flow Ctrl Lo value has a valid range from 1 to 510 and must be lower than the Flow Ctrl Hi value.

This value sets the flow control threshold for sending the signal to the attached Ethernet device to resume transmission.

d. In the Flow Ctrl Hi column, click the cell in the row for the appropriate port.

e. Enter a value in the cell. The Flow Ctrl Hi value has a valid range from 2 to 511 and must be higher than the Flow Ctrl Lo value.

This value sets the flow control threshold for sending the signal to the attached Ethernet device to pause transmission.

f. Click **Apply**.

Note Low watermarks are optimum for low latency subrate applications, such as voice-over-IP (VoIP) using an STS-1. High watermarks are optimum when the attached Ethernet device has insufficient buffering, best effort traffic, or long access line lengths.

Step 6 Return to your originating procedure (NTP).

NTP-A241 Provision G-Series Ports for Transponder Mode

Purpose	This procedure provisions G-Series ports into transponder mode.
Tools/Equipment	None
Prerequisite Procedures	A222 Provision G-Series Ethernet Ports, page 86
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will provision G-Series ports. If you are already logged in, continue with Step 2.

Step 2 In the node view, double-click the G-Series card graphic to open the card.

Step 3 Click the **Provisioning** > **Port** tabs.

Step 4 To put a pair of G-Series card ports in two-port bidirectional transponder mode (Figure 8-15):

In this step, "Port A" represents the first port in a pair and "Port B" the second port in the pair. You can pair any two ports on a G-Series card in two-port bidirectional mode.

a. Click the Port A row (for example, Port 1).

b. In the TXP Mode column, choose **TX/RX** from the drop-down menu.

c. In the TXP Port column, choose the port number that reflects Port A (for example, Port 1).

d. Click a Port B row (for example, Port 2).

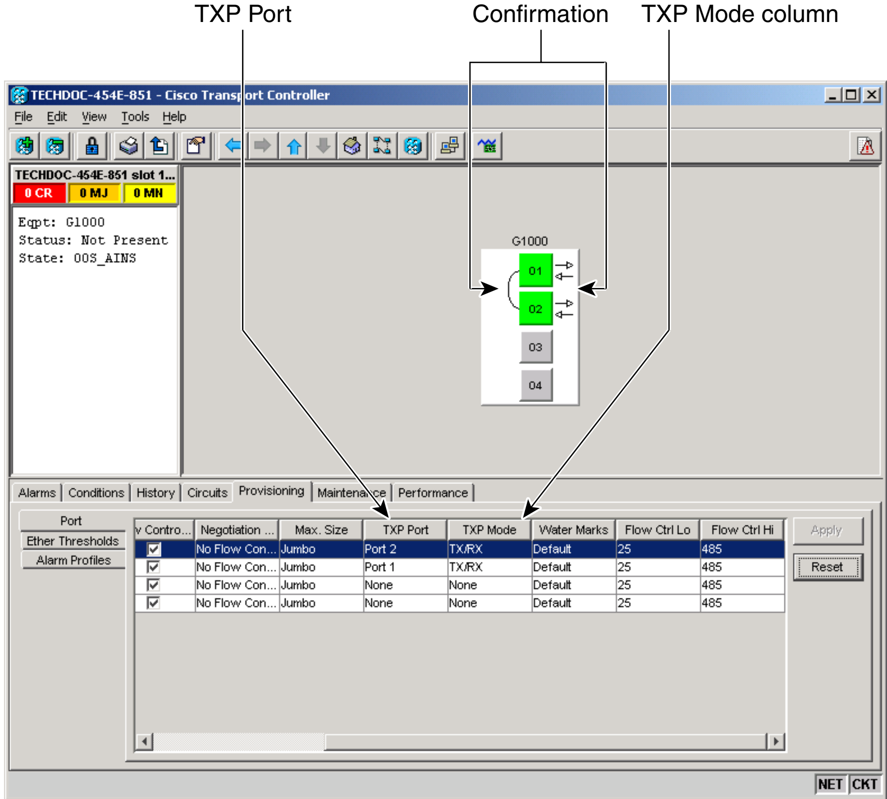
e. In the TXP Mode column, choose **TX/RX** from the drop-down menu.

f. In the TXP Port column, choose Port A (for example, Port 1) from the drop-down menu.

g. Click **Apply**.

The ports in the card view have arrows and a connecting line between the back of the ports.

Figure 8-15 Two-Port Bidirectional Transponder Mode



Step 5 To put a G-Series card port in one-port bidirectional transponder mode (Figure 8-16):

a. Click the desired port row (for example, Port 1).

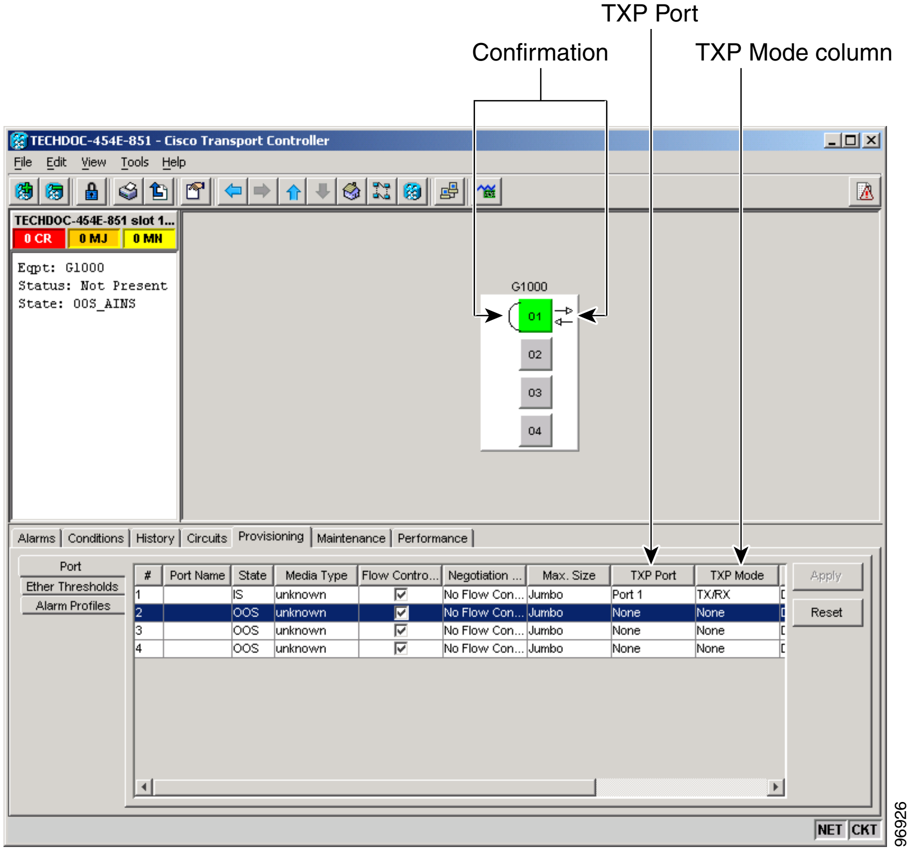
b. In the TXP Mode column, choose **TX/RX** from the drop-down menu.

c. In the TXP Port column, choose the desired port from the drop-down menu (for example, Port 1).

d. Click **Apply**.

In card view, the desired port has arrows and a curved line on the back of the port.

Figure 8-16 One-Port Bidirectional Transponder Mode



#	Port Name	State	Media Type	Flow Contro...	Negotiation ...	Max. Size	TXP Port	TXP Mode
1		IS	unknown	☑	No Flow Con...	Jumbo	Port 1	TX/RX
2		OOS	unknown	☑	No Flow Con...	Jumbo	None	None
3		OOS	unknown	☑	No Flow Con...	Jumbo	None	None
4		OOS	unknown	☑	No Flow Con...	Jumbo	None	None

Step 6 To provision two-port unidirectional transponder mode (Figure 8-17):

In this step, "Port A" represents the first port in a pair and "Port B" the second port in the pair. You can pair any two ports on a G-Series card in two-port unidirectional mode.

a. Click the Port A row (for example, Port 1).

b. Uncheck Flow Control Neg. Ports cannot be provisioned in unidirectional transponder mode when autonegotiation is enabled.

c. In the TXP Port column, choose Port B (for example, Port 2) from the drop-down menu.

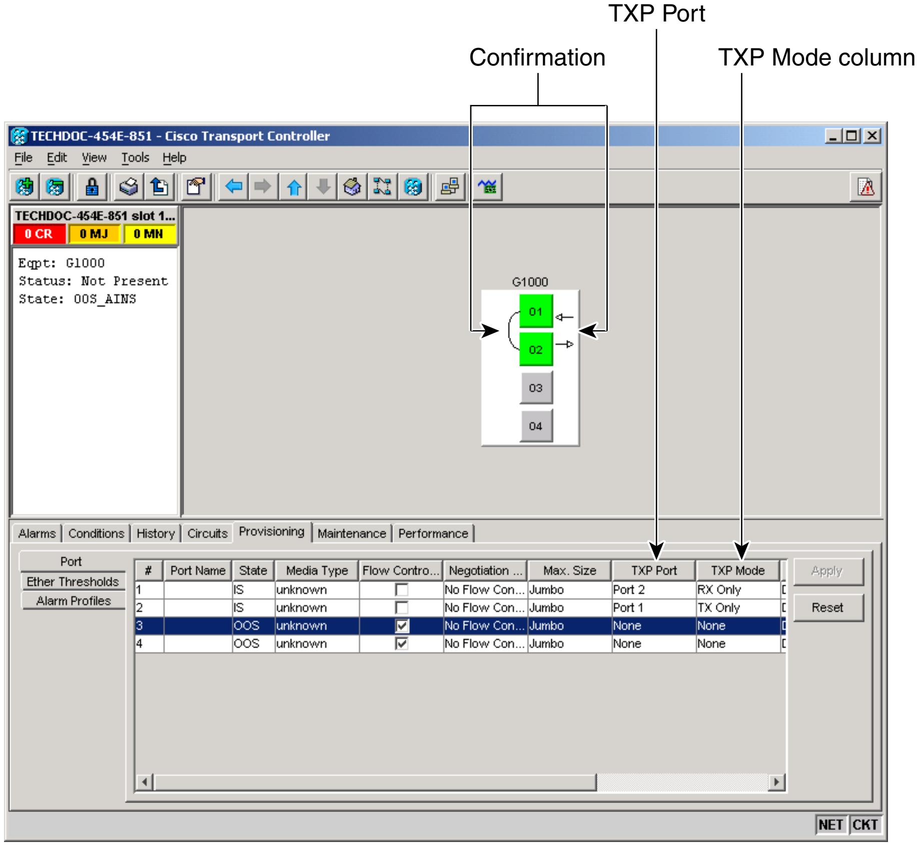
d. In the TXP Mode column, choose **RX Only** from the drop-down menu. CTC completes the Port B TXP Port with Port A and TXP Mode with TX Only.

e. Click the Port B row and uncheck Flow Control Neg.

f. Click **Apply**.

The ports on the CTC card level view display arrows and a line between the back of the ports.

Figure 8-17 Two-Port Unidirectional Transponder Mode



Stop. You have completed this procedure.

NTP-A149 Test G-Series Circuits

Purpose	This procedure tests circuits created on G-Series cards.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15454s to the fiber distribution panel or the DSX, and one of the following: NTP-A147 Create a G-Series STS Circuit, page 8-82 NTP-A148 Create a Manual Cross-Connect for a G-Series or E-Series Card in Port-Mapped Mode, page 8-84
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit.

Step 2 Change the circuit and circuit ports to an OOS-MT service state:

a. Click the **Circuits** tab.

b. Click the circuit you want to test.

c. From the Tools menu, choose **Circuits > Set Circuit State**.

d. In the Set Circuit State dialog box, choose **OOS_MT** from the Target Circuit State drop-down menu.

e. Check the **Apply to drop ports** check box.

f. Click **OK**.

Step 3 On the shelf graphic, double-click the circuit source card.

Step 4 Click the **Provisioning > Port** tabs.

Step 5 Verify the following settings:

- State—OOS_MT
- Flow Control Neg—Checked or unchecked as indicated by the circuit or site plan
- Max Size—Checked or unchecked as indicated by the circuit or site plan
- Media Type— SX, LX, ZX, CWDM, or DWDM

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you are not able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to the SONET topology:

- For path protection configurations, complete the "DLP-A94 Path Protection Switching Test" task on page 6-40.
- For BLSRs, complete the "DLP-A91 BLSR Switch Test" task on page 6-26.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 Change the circuit and circuit ports to the IS service state:

a. Click the **Circuits** tab.

b. Choose the circuit you want to test.

c. From the Tools menu, choose **Circuits > Set Circuit State**.

d. In the Set Circuit State dialog box, choose **IS** from the Target Circuit State drop-down menu.

e. Check the **Apply to drop ports** check box.

f. Click **OK**.

Step 12 After the circuit test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results, see your test set user guide.

Stop. You have completed this procedure.

NTP-A194 Create Overhead Circuits

Purpose	This procedure creates overhead circuits on an ONS 15454 network. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, the AIC and AIC-I card orderwire, and the AIC-I card user data channel.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the overhead circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 As needed, complete the "DLP-A313 Create a DCC Tunnel" task on page 8-93.

Step 4 As needed, complete the "DLP-A341 Create an IP-Encapsulated Tunnel" task on page 8-95.

Step 5 As needed, complete the "DLP-A83 Provision Orderwire" task on page 8-96.

Step 6 As needed, complete the "DLP-A212 Create a User Data Channel Circuit" task on page 8-97.

Stop. You have completed this procedure.

DLP-A313 Create a DCC Tunnel

Purpose	This task creates an DCC tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. Tunnels can be created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC), or any Line DCC channel (D4-D6, D7-D9, or D10-D12).
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends a maximum of 84 DCC tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as a DCC tunnel endpoint, and a Section DCC that is used as an DCC tunnel endpoint cannot be terminated. All DCC tunnel connections are bidirectional.

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Circuit Type—Choose one:
  - DCC Tunnel-D1-D3—Allows you to choose either the Section DCC (D1-D3) or a Line DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
  - DCC Tunnel-D4-D12—Provisions the full Line DCC as a tunnel.

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—This is the Section DCC.
  - DCC2 (D4-D6)—This is Line DCC 1.
  - DCC3 (D7-D9)—This is Line DCC 2.
  - DCC4 (D10-D12)—This is Line DCC 3.

  DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—This is the Section DCC.
  - DCC2 (D4-D6)—This is Line DCC 1.
  - DCC3 (D7-D9)—This is Line DCC 2.
  - DCC4 (D10-D12)—This is Line DCC 3.

  DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.

Step 8 Click **Finish**.

Step 9 Put the ports that are hosting the DCC tunnel in service. See the "DLP-A214 Change the Service State for a Port" task on page 6-6 for instructions.

Step 10 Return to your originating procedure (NTP).

DLP-A341 Create an IP-Encapsulated Tunnel

Purpose	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. IP-encapsulated tunnels are created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC).
Tools/Equipment	None
Prerequisite Procedures	NTP-A35 Verify Node Turn Up, page 6-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15454 can have up to ten IP-encapsulated tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as a tunnel endpoint, and a Section DCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

Step 1 Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the "DLP-A249 Provision IP Settings" task on page 4-10.

Step 2 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click **Create**.

Step 4 In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Type—Choose **IP Tunnel-D1-D3**.
- Maximum Bandwidth—Type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).

Step 5 Click **Next**.

Step 6 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—Displays IPT (D1-D3).

Step 7 Click **Next**.

Step 8 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—Displays IPT (D1-D3).

Step 9 Click **Finish**.

Step 10 Put the ports that are hosting the IP-encapsulated tunnel in service. See the "DLP-A214 Change the Service State for a Port" task on page 6-6 for instructions.

Step 11 Return to your originating procedure (NTP).

DLP-A83 Provision Orderwire

Purpose	This task provisions orderwire on the AIC or the AIC-I card.
Tools/Equipment	An AIC or AIC-I card must be installed in Slot 9.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Circuit Type—Choose either **Local Orderwire** or **Express Orderwire** depending on the orderwire path that you want to create. If regenerators are not used between ONS 15454 nodes, you can use either local or express orderwire channels. If regenerators exist, use the express orderwire channel. You can provision up to four ONS 15454 OC-N ports for each orderwire path.
- PCM—Choose the Pulse Code Modulation voice coding and companding standard, either Mu_Law (North America, Japan) or A_Law (Europe). The provisioning procedures are the same for both types of orderwire.

Caution When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

For non-DWDM nodes, the slots and ports are OC-N cards. For DWDM nodes, the slots and ports are OSC cards.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.

- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.

For non-DWDM nodes, the slots and ports are OC-N cards. For DWDM nodes, the slots and ports are OSC cards.

Step 8 Click **Finish**.

Step 9 Return to your originating procedure (NTP).

DLP-A212 Create a User Data Channel Circuit

Purpose	This task creates a user data channel (UDC) circuit on the ONS 15454. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Type—Choose either **User Data-F1** or **User Data D-4-D-12** from the drop-down menu. (User Data D-4-D-12 is not available if the ONS 15454 is provisioned for DWDM.)

Step 4 Click **Next**.

Step 5 In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

For non-DWDM nodes, the slots and ports are OC-N cards. For DWDM nodes, the slots and ports are OSC cards.

Step 6 Click **Next**.

Step 7 In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.

Step 8 Click **Finish**.

Step 9 Return to your originating procedure (NTP).

NTP-A227 Provision a DWDM Optical Channel Network Connection

Purpose	This procedure creates an optical channel network connection (OCHNC) between ONS 15454s that are provisioned for DWDM.
Tools/Equipment	DWDM optical passive units (32 MUX-0, 32 DMX-0, 4MD-xx.x) and OADM (band or channel) cards must be installed at the nodes within the OCHNC route.
Prerequisite Procedures	NTP-A232 Verify DWDM Node Turn Up, page 7-2 NTP-A280 Provision DWDM or Hybrid Network Connections, page 7-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the DWDM OCHNC. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the OCHNC source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

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

Step 5 In the Circuit Creation dialog box, choose **OCHNC** from the Circuit Type list.

Step 6 Click **Next**.

Step 7 Define the circuit attributes:

- Name—Assign a name to the OCHNC. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—Choose one of the following options depending upon whether a TXP_MR_10G, MXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card is connected to the OCHNC end points:
  - Equipped non specific—Choose this option if you do not know which card will be installed at the OCHNC end points.
  - Multi-rate—Choose this option if a TXP_MR_2.5G or TXPP_MR_2.5G card that is provisioned for Fiber Channel, Gigabit Ethernet, or ESCON (Enterprise Systems Connection) is connected to the OCHNC end points.
  - 2.5 Gb/s No FEC— Choose this option if a TXP_MR_2.5G or TXPP_MR_2.5G card that is not provisioned for forward error correction (FEC) is connected to the OCHNC end points.
  - 2.5 Gb/s FEC—Choose this option if a TXP_MR_2.5G or TXPP_MR_2.5G card that is provisioned for FEC is connected to the OCHNC end points.

- 10 Gb/s No FEC—Choose this option if a TXP_MR_10G or MXP_MR_10G card that is not provisioned for FEC is connected to the OCHNC end points.
- 10 Gb/s FEC—Choose this option if a TXP_MR_10G or MXP_MR_10G card that is provisioned for FEC is connected to the OCHNC end points.

- OCHNC Channel—Choose the wavelength you want to provision. Thirty-two wavelengths are available. See Table 5-6 on page 5-20 for a list of OADM channels.
- OCHNC Direction—Choose the line direction, either West to East to East to West. By default, West refers to ports located in Slots 1 to 7, and East refers to the ports located in Slots 11 to 17.
  - West to East—West is the receive (Rx) path and east is the transmit (Tx) path
  - East to West—East is the Rx path and west is the Tx path
- Bidirectional—Check this check box to create a bidirectional OCHNC; uncheck it to create a unidirectional OCHNC.

Step 8 Click **Next**.

Step 9 In the Circuit Source area, choose the source node from the Node drop-down menu.

Step 10 Click **Next**.

Step 11 In the Circuit Destination area, choose the destination node from the Node drop-down menu.

Step 12 Click **Finish**.

Stop. You have completed this procedure.

NTP-A264 Create an Automatically Routed VCAT Circuit

Purpose	This procedure creates an automatically routed VCAT circuit.
Tools/Equipment	ML-Series or FC_MR-4 cards must be installed at the nodes used in the VCAT circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note You can provision a maximum of two VCAT circuits for ML-Series cards.

Note For FC_MR-4 cards with a line rate 2-Gbps fiber channel, an equivalent VCAT circuit does not exist. A contiguous STS-48c circuit is used instead. FC_MR-4 cards with a line rate 1-Gbps fiber channel use eight VCAT members, each member using an STS-3c or STS-24c circuit. Software Release 4.6 supports line rate connections, not subrate connections. As a result, you cannot change the rate from 1-Gbps to 2-Gbps if the circuit rate is STS-24c.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the VCAT circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab, then click **Create**.

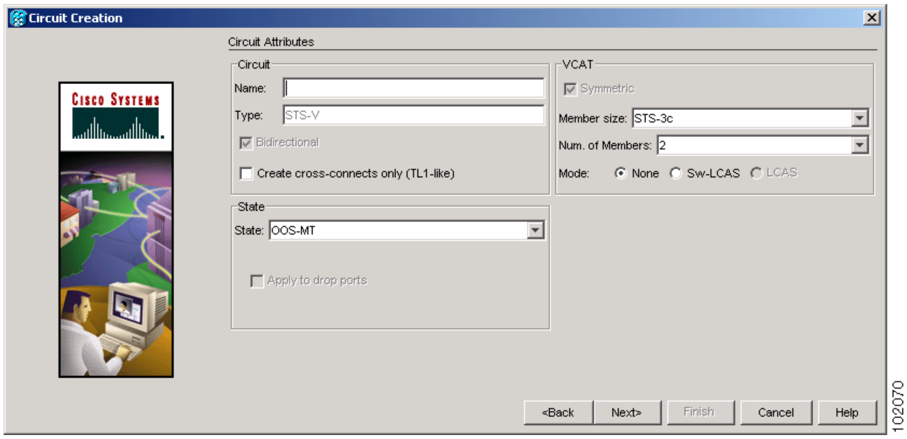
Step 4 In the Circuit Creation dialog box, choose **STS-V** from the Circuit Type drop-down menu.

Step 5 Click **Next**.

Step 6 Define the circuit attributes (Figure 8-18 on page 8-101):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Displays the circuit type you chose in Step 4. You cannot change it.
- Bidirectional—Checked is the default. You cannot change it.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Not applicable.
- Symmetric—Checked is the default. You cannot change it.
- Member size—Choose the member size: STS-1c, STS-3c, or STS-12c. For FC_MR-4 cards, only STS-3c is available.
- Num. of members—For VCAT circuits on FC_MR-4 cards, choose **8**. For VCAT circuits on ML-Series cards, choose **2**.
- Mode—Choose the protection mode for the VCAT circuit:
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail.
  - Sw-LCAS—Allows the VCAT circuit to adapt to member failures and keep traffic flowing after failures at a reduced bandwidth.

Figure 8-18 Setting VCAT Circuit Attributes



Step 7 Click **Next**.

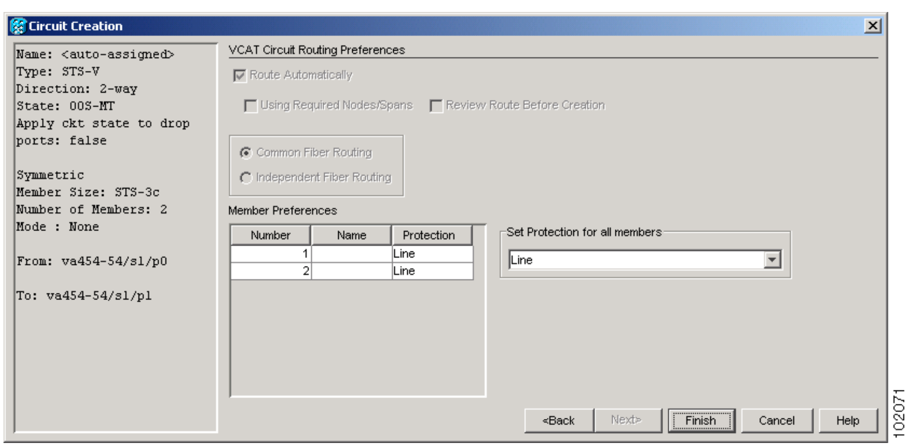
Step 8 Complete the "DLP-A324 Provision a VCAT Circuit Source and Destination" task on page 8-103 for the VCAT circuit you are creating.

Step 9 In the VCAT Circuit Routing Preferences area (Figure 8-19), check **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

Note Software Release 4.6 only supports common fiber routing, where all members travel on the same fibers.

Figure 8-19 Automatically Routing a VCAT Circuit



Step 10 In the Member Preferences area, complete the following:

- Number—Type a number (between 1 and 256) to identify the member.

- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path; path protection is not supported.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the circuit on a BLSR protection channel.
  - Set protection for all members—Allows you to choose the same protection type for all members.

Note If a member is unprotected, all members must be unprotected.

Step 11 Click **Next**. If you chose Fully Protected or PCA, click **OK** to continue. If not, continue with the next step.

Step 12 If you selected Using Required Nodes/Spans in Step 9, complete the following substeps. If not, continue with Step 13:

a. In the Circuit Route Constraints area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit is routed. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 13 If you selected Review Route Before Creation in Step 9, complete the following substeps; otherwise, continue with Step 14:

a. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

b. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 8-103 to assign the circuit route yourself.

Step 14 Click **Finish**. The Circuits window appears.

Step 15 In the Circuits window, verify that the circuit you created appear in the circuits list.

Stop. You have completed this procedure.

DLP-A324 Provision a VCAT Circuit Source and Destination

Purpose	This task provisions a VCAT circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 The Circuit Creation wizard Circuit Source panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down menu, choose the node where the circuit will originate.

Step 2 From the Slot drop-down menu, choose the slot containing the ML-Series cards or FC_MR-4 card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the menu.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS from the Port and STS menus. The Port menu is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

Step 4 Click **Next**.

Step 5 From the Node drop-down menu, choose the destination node.

Step 6 From the Slot drop-down menu, choose the slot containing the ML-Series cards or FC_MR-4 card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the menu.)

Step 7 Depending on the card selected in Step 2, choose the source port and/or STS from the Port and STS menus. The Port menu is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.

Step 8 Click **Next**.

Step 9 Return to your originating procedure (NTP).

NTP-A265 Create a Manually Routed VCAT Circuit

Purpose	This procedure creates a manually routed VCAT circuit.
Tools/Equipment	None
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 8-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision a maximum of two VCAT circuits for ML-Series cards.

Note For FC_MR-4 cards with a line rate 2-Gbps fiber channel, an equivalent VCAT circuit does not exist. A contiguous STS-48c circuit is used instead. FC_MR-4 cards with a line rate 1-Gbps fiber channel use eight VCAT members, each member using an STS-3c or STS-24c circuit.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-A314 Assign a Name to a Port" task on page 8-11. If not, continue with Step 3.

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

Step 4 In the Circuit Creation dialog box, choose **STS-V** from the Circuit Type drop-down menu.

Step 5 Click **Next**.

Step 6 Define the circuit attributes (Figure 8-18 on page 8-101):

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Displays the circuit type you chose in Step 4. You cannot change it.
- Bidirectional—Checked is the default. You cannot change it.
- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-A230 Change a Circuit State" task on page 11-13.
- Apply to drop ports—Not applicable.
- Symmetric—Checked is the default. You cannot change it.
- Member size—Choose the member size: STS-1c, STS-3c, or STS-12c. For FC_MR-4 cards, only STS-3c is available.
- Num. of members—For VCAT circuits on FC_MR-4 cards, choose **8**. For VCAT circuits on ML-Series cards, choose **2**.
- Mode—Choose the protection mode for the VCAT circuit:
  - None—Provides no protection. A failure on one member causes the entire VCAT circuit to fail.
  - Sw-LCAS—Allows the VCAT circuit to adapt to member failures and keep traffic flowing after failures at a reduced bandwidth.

Step 7 Click **Next**.

Step 8 Complete the "DLP-A324 Provision a VCAT Circuit Source and Destination" task on page 8-103 for the VCAT circuit you are creating.

Step 9 In the Circuit Routing Preferences area (Figure 8-19 on page 8-101), uncheck **Route Automatically**.

Step 10 In the Member Preferences area, complete the following:

- Number—Type a number (between 1 and 256) to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path; path protection is not supported.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the circuit on a BLSR protection channel.
  - Set protection for all members—Allows you to choose the same protection type for all members.

Note If a member is unprotected, all members must be unprotected.

Step 11 Click **Next**. If you chose Fully Protected or PCA, click **OK** to continue. If not, continue with the next step.

Step 12 In the Route Review and Edit area, node icons appear so you can route the circuit manually.

Step 13 Complete the "DLP-A325 Provision a VCAT Circuit Route" task on page 8-105.

Step 14 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path.

Step 15 When all the circuits are created, the main Circuits window appears. Verify that the circuit you created appear in the window.

Stop. You have completed this procedure.

DLP-A325 Provision a VCAT Circuit Route

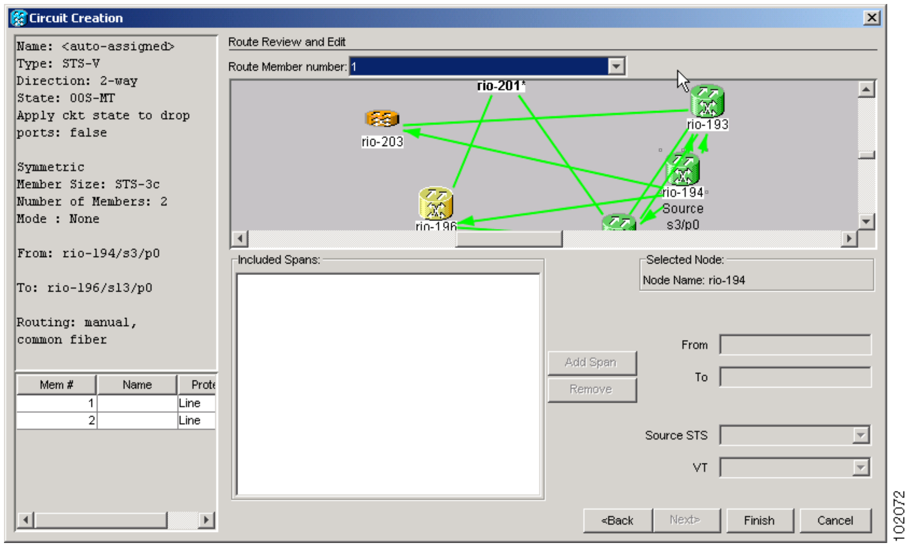
Purpose	This task provisions the circuit route for manually routed OC-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	The Circuit Creation wizard Route Review and Edit panel must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Creation wizard in the Route Review and Edit area, choose the member number from the Route Member Number drop-down menu.

Step 2 Click the source node icon if it is not already selected.

Step 3 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 8-20 shows an example.

Figure 8-20 Manually Routing a VCAT Circuit



Step 4 Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 3 and 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Repeat Steps 1 through 5 for each member.

Step 7 Return to your originating procedure (NTP).

CHAPTER 9

Manage Alarms

This chapter explains how to view and manage the alarms and conditions on a Cisco ONS 15454.

Cisco Transport Controller (CTC) detects and reports alarms generated by the Cisco ONS 15454 and the ONS network. You can use CTC to monitor and manage alarms at a card, node, or network level. You can also view alarm counts on the LCD front panel.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A195 Document Existing Provisioning, page 9-2—Complete this procedure as needed to print or export node data.
2. NTP-A196 View Alarms, History, Events, and Conditions, page 9-5—Complete this procedure as needed to see alarms and conditions occurring on the node and a complete history of alarm and condition messages.
3. NTP-A68 Delete Cleared Alarms from Display, page 9-13—Complete this procedure as needed to delete cleared alarm information.
4. NTP-A69 View Alarm-Affected Circuits, page 9-14—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port, page 9-16—Complete this procedure as needed to see a statistical count of alarms that have occurred for a slot or port.
6. NTP-A71 Create, Download, and Assign Alarm Severity Profiles, page 9-17—Complete this procedure as needed to change the default severity for certain alarms, to assign the new severities to a port, card, or node, and to delete alarm profiles.
7. NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering, page 9-29—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens at the node or network level.
8. NTP-A72 Suppress Alarms or Discontinue Alarm Suppression, page 9-33—Use these tasks as needed to suppress reported alarms at the port, card, or node level and to disable the suppress command to resume normal alarm reporting.

NTP-A195 Document Existing Provisioning

Purpose	This procedure prints card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer. It also exports card, node, or network information as delineated text files to other applications. This procedure is useful for network record keeping and troubleshooting.
Tools/Equipment	A printer connected to the CTC computer by a direct or network connection
Prerequisite Procedures	Chapter 4, "Turn Up Node"
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to record or save data. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A515 Print CTC Data" task on page 9-2.

Step 3 As needed, complete the "DLP-A516 Export CTC Data" task on page 9-4.

Stop. You have completed this procedure.

DLP-A515 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Click the tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.

The print operation is available for all network, node, and card view windows.

Step 2 From the File menu choose **Print**.

Step 3 In the Print dialog box, click a printing option (Figure 9-1).

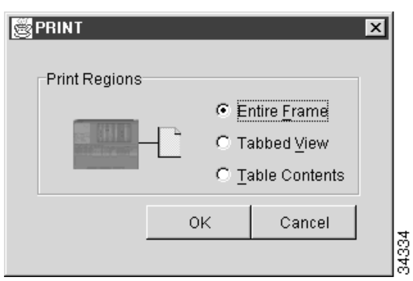
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
- Tabbed View—Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.

- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option applies to all windows except:
  - Provisioning > General > General, Power Monitor windows
  - Provisioning > Network > General, RIP windows
  - Provisioning > Security > Policy, Access, or Legal Disclaimer windows
  - Provisioning > SNMP window
  - Provisioning > Timing window
  - Provisioning > UCP > Node window
  - Provisioning > WDM-ANS> Provisioning window
  - Maintenance > Cross-Connect > Cards window
  - Maintenance > Database window
  - Maintenance > Diagnostic window
  - Maintenance > Protection window
  - Maintenance > Timing > Source window

  The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that network view does not contain an Inventory tab or Performance tab.

Figure 9-1 Selecting CTC Data For Print



Step 4 Click **OK**.

Step 5 In the Windows Print dialog box, click a printer and click **OK**.

Step 6 Repeat this task for each window that you want to print.

Step 7 Return to your originating procedure (NTP).

DLP-A516 Export CTC Data

Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

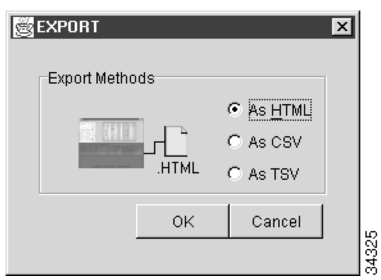
Step 1 Click the tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).

Step 2 Choose **Export from the File menu**.

Step 3 In the Export dialog box, click a data format (Figure 9-2):

- As HTML—Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
- As CSV—Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report window.
- As TSV—Saves the CTC table as tab-separated values (TSV).

Figure 9-2 Selecting CTC Data For Export



Step 4 If you want to open a file in a text editor or word processor application, procedures may vary; but typically you can use the File > Open command to view the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications format the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.

Step 5 If you want to open the file in spreadsheet and database management applications, procedures may vary; but typically you need to open the application and choose File > Import, then choose a delimited file to format the data in cells.

Spreadsheet and database management programs also allow you to manage the exported data.

Note An exported file cannot be opened in CTC.

The export operation applies to all tabular data except:

- Provisioning > General > General, Power Monitor windows
- Provisioning > Network > General, RIP windows
- Provisioning > Security > Policy, Access, or Legal Disclaimer windows
- Provisioning > SNMP window
- Provisioning > Timing window
- Provisioning > UCP > Node window
- Provisioning > WDM-ANS> Provisioning window
- Maintenance > Cross-Connect > Cards window
- Maintenance > Database window
- Maintenance > Diagnostic window
- Maintenance > Protection window
- Maintenance > Timing > Source, Report windows

Step 6 Click **OK**.

Step 7 In the Save dialog box, enter a name in the File name field using one of the following formats:

- [filename].html—for HTML files
- [filename].csv—for CSV files
- [filename].tsv—for TSV files

Step 8 Navigate to a directory where you want to store the file.

Step 9 Click **OK**.

Step 10 Repeat the task for each window that you want to export.

Step 11 Return to your originating procedure (NTP).

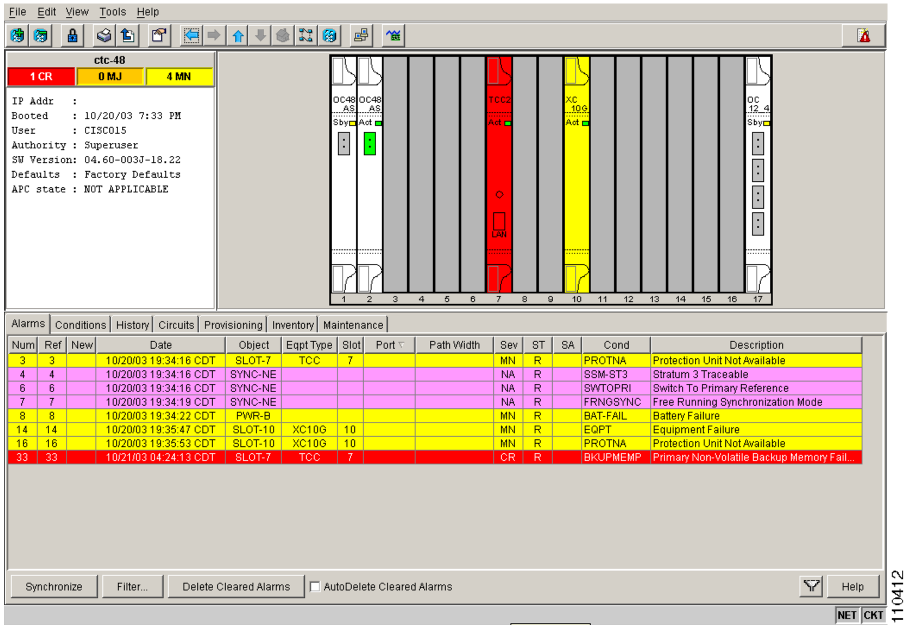
NTP-A196 View Alarms, History, Events, and Conditions

Purpose	This procedure is used to view current or historical alarms and conditions for a card, a node, or network. This information is useful for monitoring and troubleshooting hardware and software events.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that contains the alarms you want to view. If you are already logged in, continue with Step 2.

Step 2 In the card, node, or network view, click the **Alarms** tab to view the alarms for that card, node, or network (Figure 9-3).

Figure 9-3 CTC Node View



[Table 9-1](#) lists the columns in the Alarms window and their descriptions.

Table 9-1 Alarm Column Descriptions

Column	Information Recorded
New	Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button
Date	Date and time of the alarm
Node	Node where the alarm occurred (appears only in network view)
Object	TL1 access identifier (AID) for the alarmed object; for an STSmon or VTmon, this is the monitored STS or VT
Eqpt Type	If an alarm is raised on a card, the card type in this slot
Slot	If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view)
Port	If an alarm is raised on a card, the port where the alarm is raised; for STSTerm and VTTerm, the port refers to the upstream card it is partnered with
Path Width	Indicates how many STSs are contained in the alarmed path. This information compliments the alarm object notation, which is explained in Table 9-3.
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not-alarmed), NR (not-reported)
ST	Status: R (raised), C (clear)
SA	When checked, indicates a service-affecting alarm
Cond	The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15454 Troubleshooting Guide*
Description	Description of the alarm

Table 9-1 Alarm Column Descriptions (continued)

Column	Information Recorded
Num	An incrementing count of alarm messages
Ref	The reference number assigned to the alarm

Table 9-2 lists the color codes for alarm and condition severities. In addition to the severities listed in the table, CTC alarm profiles list inherited (I) and unset (U) severities. These are only listed in the network view Provisioning > Alarm Profiles tab and are not currently implemented.

Table 9-2 Color Codes for Alarms and Condition Severities

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta (pink)	Raised Not-Alarmed (NA) condition
Blue	Raised Not-Reported (NR) condition
White	Cleared (C) alarm or condition

In network view, CTC identifies STS and VT alarm objects using a TL1-type access identifier (AID). Table 9-3 lists these AIDs.

Table 9-3 Network View STS and Alarm Object Identification

STS and VT Alarm Numbering		
MON object	STS-<Slot>-<Port>-<STS> For example, STS-6-1-6 VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-1-6-1-1	Port=1
TERM object	<Upstream Slot>-<Port>-<STS> For example, STS-6-3-6 <Upstream Slot>-<Port>-<STS>-<VT Group>-<VT> For example, VT1-6-3-6-1-1	Port=1

Step 3 If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide* for information and troubleshooting procedures.

Step 4 Complete the "DLP-A517 View Alarm or Event History" task on page 9-8, the "DLP-A113 Synchronize Alarms" task on page 9-11, or the "DLP-A114 View Conditions" task on page 9-11 as needed.

Stop. You have completed this procedure.

DLP-A517 View Alarm or Event History

Purpose	This task is used to view past cleared and uncleared ONS 15454 alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Decide whether you want to view the alarm message history at the node, network, or card level.

Step 2 To view node alarm history:

a. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.

b. Click the **History > Node** tabs to view the alarm and condition history for the node.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

c. Click **Retrieve** to view all available messages for the History > Node tabs.

Note Alarms can be unreported when they are filtered out of the display using the Filter button in either tab. See the "DLP-A225 Enable Alarm Filtering" task on page 9-29 for information.

Tip Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Step 3 To view network alarm history, from node view:

a. From the **View menu choose Go to Network View**.

b. Click the **History** tab.

Alarms and conditions (events) raised during the current session appear.

Step 4 To view card alarm history from node view:

a. From the View menu choose **Go to Previous View**.

b. Double-click a card on the shelf graphic to open the card-level view.

Note TCC2 cards and cross-connect (XC or XC10G) cards do not have a card view.

c. Click the **History > Session** tab to view the alarm messages raised during the current session.

d. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

Note The ONS 15454 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15454 discards the oldest events in that category.

Raised and cleared alarm messages (and events, if selected) appear.

Step 5 Return to your originating procedure (NTP).

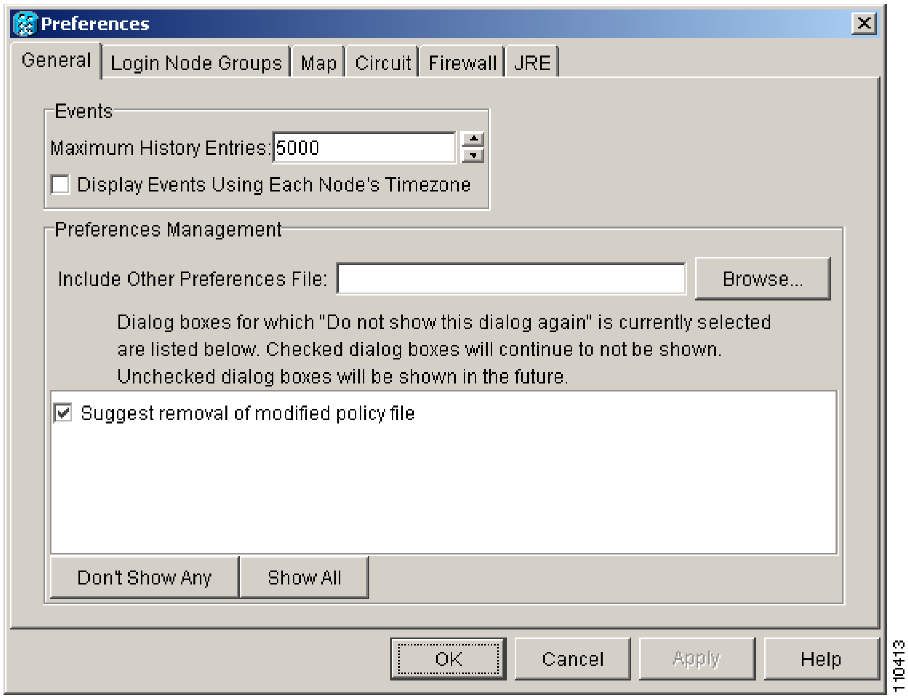
DLP-A111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 From the Edit menu, choose **Preferences**.

The CTC Preferences dialog box appears (Figure 9-4).

Figure 9-4 CTC Preferences Dialog Box



Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.

> **Note** Setting the Maximum History Entries value to the high end of the range uses more CTC memory and could impair CTC performance.

> **Note** This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-A112 Display Alarms and Conditions Using Time Zone

Purpose	This task changes the timestamp for events to the timezone of the ONS node reporting the alarm. By default, the events timestamp is set to the timezone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 From the Edit menu, choose **Preferences**.

The CTC Preferences dialog box appears (Figure 9-4 on page 9-10).

Step 2 Check the **Display Events Using Each Node's Timezone** check box. The Apply button is enabled.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-A113 Synchronize Alarms

Purpose	This task is used to view ONS 15454 events at the card, node, or network level and to refresh the alarm listing so that you can check for new and cleared alarms and conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the card, node, or network view, click the **Alarms** tab.

Step 2 Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as raise/clear messages arrive from the node.

Note Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

Step 3 Return to your originating procedure (NTP).

DLP-A114 View Conditions

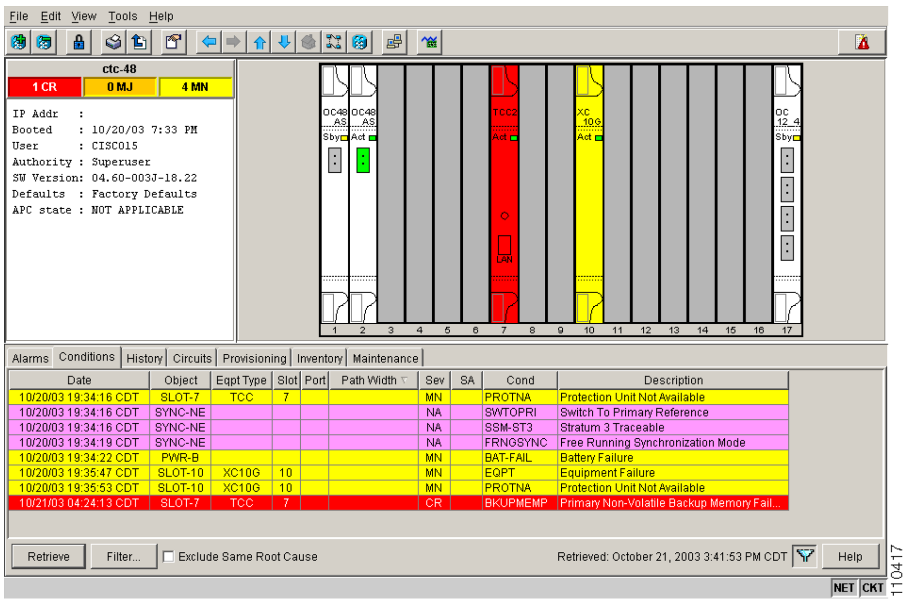
Purpose	This task is used to view conditions [events with a Not-Reported (NR) severity] at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 From the card, node, or network view, click the **Conditions** tab.

Step 2 Click **Retrieve** (Figure 9-5).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when events change on the node. You must click Retrieve to see any changes.

Figure 9-5 Node View Conditions Window



Conditions include all fault conditions raised on the node, whether or not they are reported.

Note Alarms can be unreported when they are filtered out of the display. See the "DLP-A225 Enable Alarm Filtering" task on page 9-29 for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not-Alarmed (NA) are conditions. Conditions that are not reported at all are marked Not-Reported (NR) in the Conditions window severity column.

Conditions that have a default severity of Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA) but are not reported due to exclusion or suppression are shown as NR in the Conditions window.

Note For more information about alarm suppression, see the "DLP-A522 Suppress Alarm Reporting" task on page 9-33.

Current conditions are shown with the severity chosen in the alarm profile, if used. For more information about alarm profiles, see the "NTP-A71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 9-17.

Note When a port is placed in the out of service for maintenance (OOS-MT) state, it raises an Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Note When a port is placed in out of service/auto in-service state but is not connected to a valid signal, it generates a loss of signal (LOS) alarm.

Step 3 If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.

An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break may cause an LOS alarm, an AIS condition, and an SF condition. If you check the Exclude Same Root Cause check box, only the LOS alarm will appear. According to Telcordia, exclusion rules apply to a query of "all conditions from a node."

Step 4 Return to your originating procedure (NTP).

NTP-A68 Delete Cleared Alarms from Display

Purpose	This procedure deletes Cleared (C) status alarms from the alarms window. The procedure can be used to delete transient messages from the CTC History window.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node where you want to delete alarms. If you are already logged in, go to Step 2.

Step 2 To delete cleared node-level alarms:

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

b. Click **Delete Cleared Alarms**, referring to the rules in Step 5.

This action removes any cleared ONS 15454 alarms from the Alarms tab. The rows of cleared alarms turn white and have a C in their status (ST) column (Figure 9-5 on page 9-12).

Step 3 To delete cleared card-level alarms:

a. In the node view, double-click the card graphic for the card you want to open.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the rules in Step 5.

Step 4 To delete cleared network-level alarms:

a. In the node view click **View > Go to Network View**.

b. Click the **Alarms** tab and then click **Delete Cleared Alarms**, referring to the rules in Step 5.

Step 5 Consult the following rules when deleting cleared alarms:

- If the Autodelete Cleared Alarms check box is checked, an alarm disappears from the window when it is cleared.
- If the Autodelete Cleared Alarms check box is not checked, an alarm remains in the window when it is cleared. The alarm appears white in the window and has a Clear (CL) severity. The alarm can be removed by clicking the Delete Cleared Alarms button.

Step 6 To remove the transient messages from the History window, click **Delete Cleared Alarms**. Transient messages are single messages, not raise-and-clear pairs (that is, they do not have companion messages stating they are cleared).

Stop. You have completed this procedure.

NTP-A69 View Alarm-Affected Circuits

Purpose	This procedure is used to view all circuits, if any, affected by an alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	NTP-A196 View Alarms, History, Events, and Conditions, page 9-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

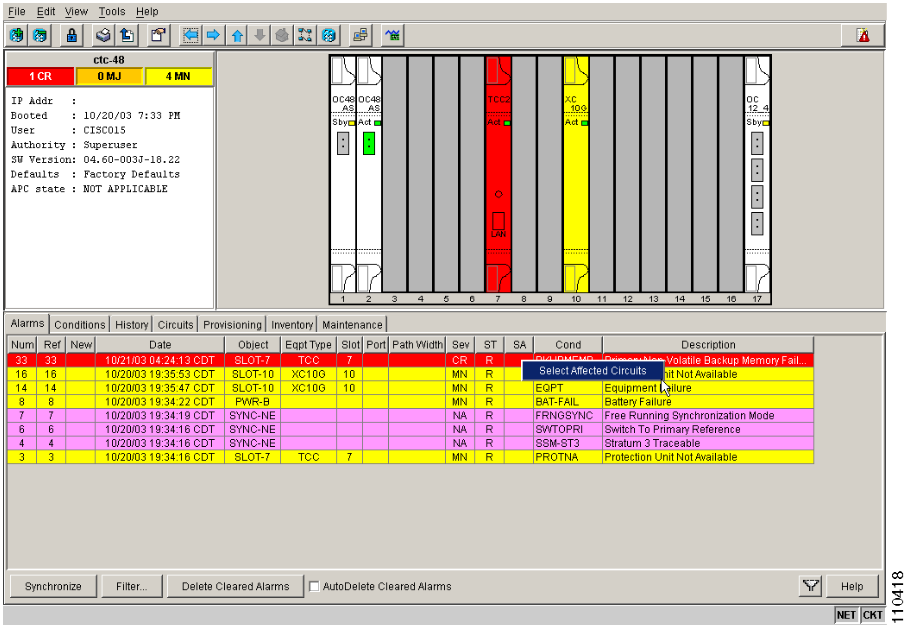
Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 In the network, node, or card view, click the **Alarms** tab or **Conditions** tab and then right-click anywhere in the row of an active alarm or condition.

Note The node view is the default, but you can also navigate to the Alarms tab in the network view or card view to perform Step 2.

The Select Affected Circuits option appears on the shortcut menu (Figure 9-6).

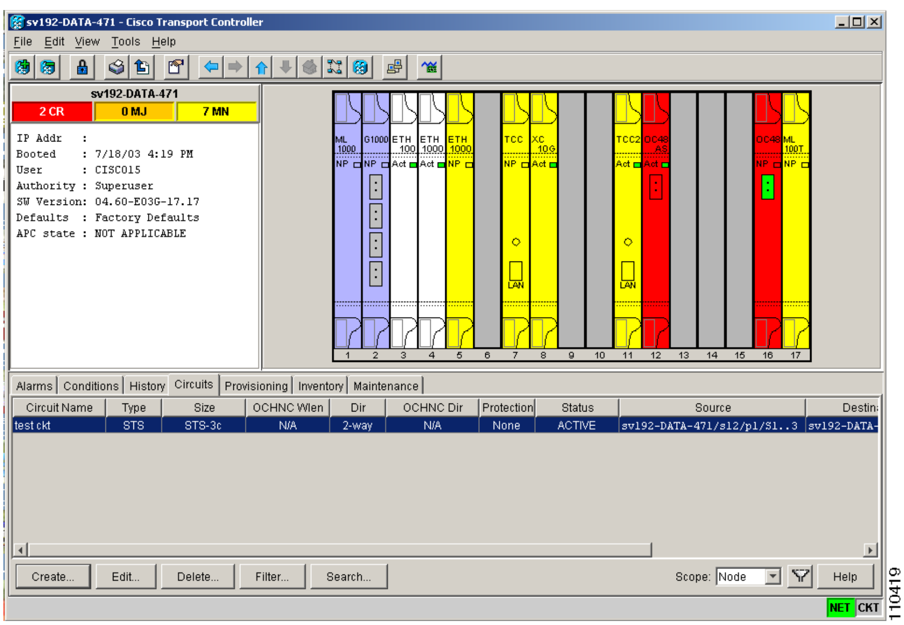
Figure 9-6 Select Affected Circuits Option



Step 3 Left-click or right-click **Select Affected Circuits**.

The **Circuits** window appears with the affected circuits highlighted (Figure 9-7).

Figure 9-7 Viewing Alarm-Affected Circuits



In Release 4.6, Select Affected Circuits behaves differently according to card types, as listed in Table 9-4.

Table 9-4 Select Affected Circuits Behavior by Alarm Type

Alarm Type	Behavior
Transient alarms (such as BLSROSYNC)	CTC displays all circuits on the node.
BITS alarms (such as SWTOSEC) Synchronization alarms (such as SYNCSEC)	CTC displays all circuits on node that the BITS or synchronization alarm reported.
Trunk card path alarms (such as AIS-P, LOP-P, or UNEQ-P)	CTC displays all circuits traversing the trunk card.
OC-N card EQPT alarms (such as IMPROPRMVL)	CTC displays no circuits.
I/O card facility, line, and path alarms (such as LPBKFACILITY, RFI-L, and PLM-P)	CTC displays only the affected circuit.

Step 4 If you want to search for particular circuits, see the "DLP-A131 Search for Circuits" task on page 11-6.

Stop. You have completed this procedure.

NTP-A70 View Alarm Counts on the LCD for a Node, Slot, or Port

Purpose	This procedure shows how many alarms have occurred on a node, slot, or port without using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 If you want to view the entire alarm summary for the node, press either the **Slot** button or **Port** button on the LCD panel until "Node" appears on the LCD. You will also see the direction, "Status=Alm Ct." This means that if you press the Status button at this time, as directed in Step 2, you will see an alarm count for the node.

Step 2 Press the **Status** button. You will see a message similar to, "Alm CT: 2: MJ:2 MN:2," meaning there are two critical alarms, two major alarms, and two minor alarms.

Step 3 If you want to see alarm counts for a particular slot, such as the alarms for an OC-3 card in slot 2, press the **Slot** button until you see "Slot-3" on the LCD. You will also see the direction, "Status=Alm Ct."

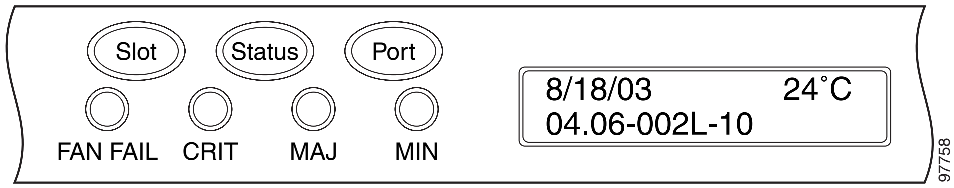
Step 4 Press the **Status** button to see a summary of alarms and severities against the slot. For example, you might see, "Slot-3 Alm CT:0 MJ:1 MN:2," meaning there are no critical alarms against the slot; there is one major alarm, and there are two minor alarms against it.

Step 5 If you want to view the alarms against a port on the card, such as Port 3 of the OC-3 card you viewed previously, press Port until you see "Port-3 Status=Alm Ct."

Step 6 Press **Status** to view alarm count against the port. You will see a message similar to, "Port-3 Alm CT:0 MJ:1 MN:0." This means that there is one major alarm against this port.

Figure 9-8 shows the shelf LCD panel.

Figure 9-8 Shelf LCD Panel



To return to the previous view from the Port screen, continue to press **Port** until the display cycles through all the ports on the slot. For instance, on the OC-3 card, press Port until it cycles past Slot 4 and you see "Slot."

To return to the node menu from the Slot screen, press **Slot** until you cycle through all the slots and see "Node."

If you do not press any buttons, the LCD will return to its default display with the node name. However, if you did not cycle through the options to return to the node status, you will see the slot or port where you last checked status.

Note A blank LCD results when the fuse on the AIP board has blown. If this occurs, log into http://www.cisco.com/tac for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of Cisco TAC toll-free numbers for your country.

Stop. You have completed this procedure.

NTP-A71 Create, Download, and Assign Alarm Severity Profiles

Purpose	This procedure creates a customized alarm profile at the network, node, or card level; assigns custom severities individually to port, card, or node, and deletes alarm profiles.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to create an alarm profile. If you are already logged in, continue with Step 2 to create, clone or modify an alarm profile, or go to Step 3 to download an alarm profile.

Step 2 Complete the "DLP-A518 Create a New or Cloned Alarm Severity Profile" task on page 9-18. This task clones a current alarm profile, renames the profile, and customizes the new profile.

Step 3 Complete the "DLP-A524 Download an Alarm Severity Profile" task on page 9-22. This task downloads an alarm severity profile from a CD or a node.

Note After storing a created or downloaded alarm profile, you must go to the node (either by logging into it or clicking on it from the network view) and activate the profile by applying it to the shelf, one or more cards, or one or more ports.

Step 4 As necessary, complete the "DLP-A519 Apply Alarm Profiles to Ports" task on page 9-24 or the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 9-26.

Stop. You have completed this procedure.

DLP-A518 Create a New or Cloned Alarm Severity Profile

Purpose	This task creates a custom severity profile or clones and modifies the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs. Figure 9-8 on page 9-19 shows the network view.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs. The node view is shown in Figure 9-3 on page 9-6.

Step 3 To access the profile editor from a card view, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SONET ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.

- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 If you want to create a new profile based upon the default profile in use, click **New**. Then go to Step 10.

Step 5 If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 7.

Step 6 If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in GR-253-CORE.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The alarm severity profile appears in the Alarm Profiles window.

Note The alarm profile list contains a master list of alarms that is used for a mixed node network. Some of these alarms may not be used in all ONS nodes.

Step 8 Right-click anywhere in the profile column to view the profile editing shortcut menu. (Refer to Step 12 for further information about the Default profile.)

Step 9 Click **Clone** in the shortcut menu.

Tip To see the full list of profiles, including those available for loading or cloning, click Available. You must load a profile before you can clone it.

Step 10 In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field.

Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported.

Step 11 Click **OK**.

A new alarm profile (named in Step 10) is created. This profile duplicates the default profile severities and appears at the right of the previous profile column in the Alarm Profiles window. You can select it and drag it to a different position.

Note Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

The Default profile sets severities to standard Telcordia GR-253-CORE settings. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the higher level. For example, if you choose the Inherited profile from the network view, the severities at the lower levels (node, card and port) will be copied from this selection. A card with an Inherited alarm profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at any level. To do this, refer to the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 9-26.)

Step 12 Modify (customize) the new alarm profile:

a. In the new alarm profile column, click the alarm severity you want to change in the custom profile.

b. Choose a severity from the drop-down menu.

c. Repeat Steps a and b for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:

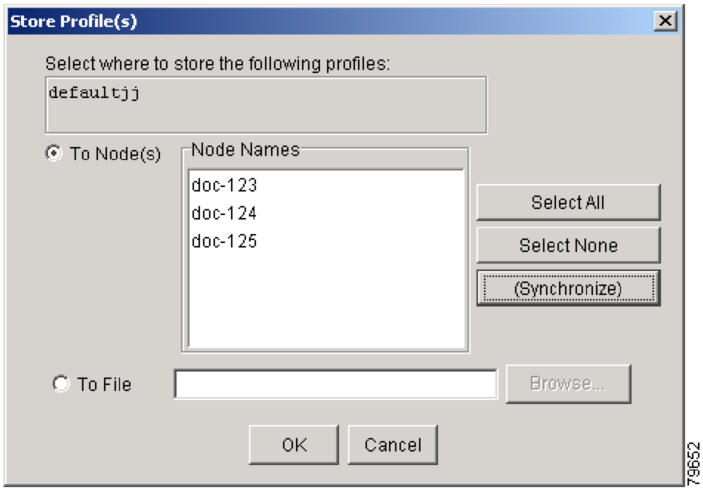
   - All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
   - Default severities are used for all alarms and conditions until you create and apply a new profile.
   - Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

Step 13 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 14 Click **Store**.

Step 15 In the Store Profile(s) dialog box, click **To Node(s)** and go to Step a or click **To File** and go to Step b (Figure 9-9).

Figure 9-9 Store Profiles Dialog Box



a. Choose the node(s) where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click **(Synchronize)**.

b. Save the profile:

- Click **Browse** and navigate to the profile save location.
- Enter a name in the File name field.
- Click **Select** to choose this name and location.

Note Long file names are supported. CTC supplies a suffix of *.pfl to stored files.

- Click **OK** to store the profile.

Note Click the Hide Identical Rows check box to configure the Alarm Profiles window to view rows with dissimilar severities.

Note Click the **Hide Reference Values** check box to configure the Alarm Profiles window to view severities that do not match the Default profile.

Note Click the Only show service-affecting severities check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.

Step 16 Return to your originating procedure (NTP).

DLP-A524 Download an Alarm Severity Profile

Purpose	This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 To access the profile editor from a card view, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports (“Ether alarming”) or packet over SONET (“POS alarming”). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click **Load**.

Step 5 If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of the profile in the Profile Names list, such as **Default**.

Step 6 If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

Note The Default alarm profile list contains alarm and condition severities that correspond when applicable to default values established in GR-253-CORE.

Note All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

Step 7 Click **OK**.

The downloaded profile appears at the right side of the Alarm Profiles window.

Step 8 Right-click anywhere in the downloaded profile column to view the profile editing shortcut menu.

Step 9 Click **Store**.

Step 10 In the Store Profile(s) dialog box, click **To Node(s)**.

a. Choose the node(s) where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click **Synchronize**.

b. Click **OK**.

Step 11 Return to your originating procedure (NTP).

DLP-A519 Apply Alarm Profiles to Ports

Purpose	This task applies a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 9-18 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click a card to open the card view.

> **Note** You can also apply alarm profiles to cards using the "DLP-A117 Apply Alarm Profiles to Cards and Nodes" task on page 9-26.

> **Note** The card view is not available for the TCC2 or cross-connect cards.

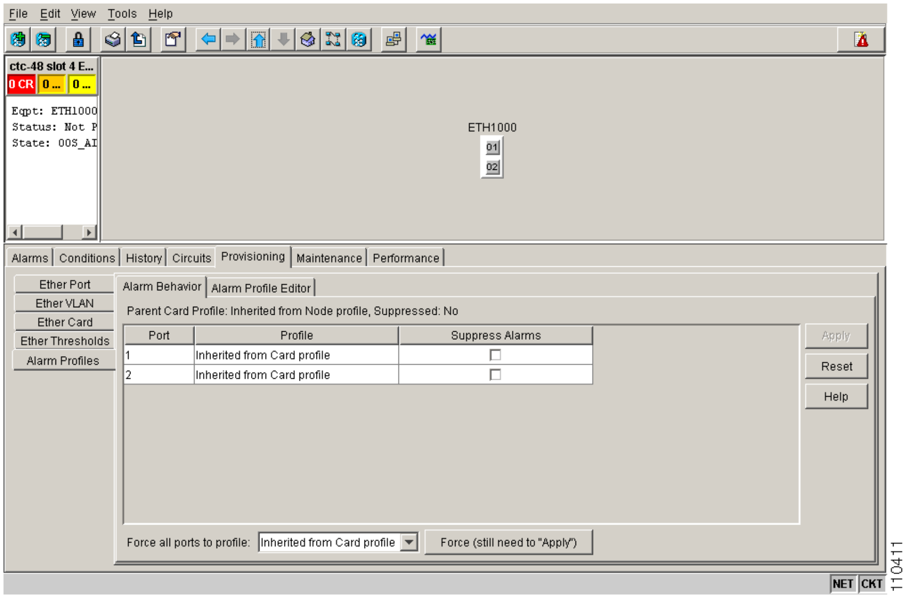
Step 2 Depending on which card you want to apply the profile to, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SONET ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.

- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Figure 9-10 shows the alarm profile of Ethernet card ports. CTC shows Parent Card Profile: Inherited.

Figure 9-10 E1000-4 Card Alarm Profile



Go to Step 3 to apply profiles to a port. Go to Step 4 to apply profiles to all ports on a card.

Step 3 To apply profiles on a port basis:

a. In card view, click the port row in the Profile column.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

Step 4 To apply profiles to all ports on a card:

a. In card view, click the **Force all ports to profile** menu arrow at the bottom of the window.

b. Choose the new profile from the drop-down list.

c. Click **Force (still need to "Apply").**

d. Click **Apply**.

In node view the Port Level Profiles column indicates port-level profiles with a notation such as "exist (1)"(Figure 9-11 on page 9-26).

Step 5 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 6 Return to your originating procedure (NTP).

DLP-A117 Apply Alarm Profiles to Cards and Nodes

Purpose	This task applies a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A518 Create a New or Cloned Alarm Severity Profile, page 9-18 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tab (Figure 9-11).

Figure 9-11 Node View Alarm Profile

Step 2 To apply profiles to a card:

a. Click the Profile row for the card.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

Step 3 To apply the profile to an entire node:

a. Click the **Node Profile** menu arrow at the bottom of the window (Figure 9-11).

b. Choose the new alarm profile from the drop-down menu.

c. Click **Apply**.

Step 4 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 5 Return to your originating procedure (NTP).

DLP-A520 Delete Alarm Severity Profiles

Purpose	This task deletes a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

Step 2 To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 3 To access the profile editor from a card view, click the following tabs:

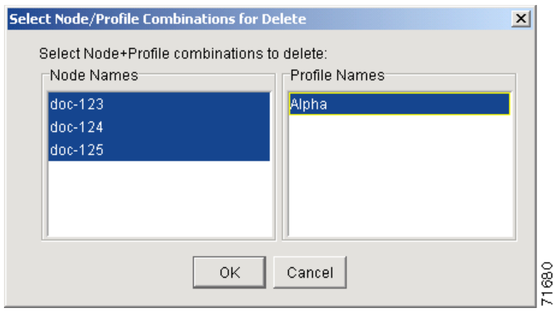
- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profile Editor** tabs or the **Provisioning > POS Alarming > Alarm Profile Editor** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SONET ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profile Editor** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles >Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profile Editor** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profile Editor** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

Step 4 Click the profile you are deleting to select it.

Step 5 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 9-12).

Figure 9-12 Select Node/Profile Combination For Delete Dialog Box



Note You cannot delete the Inherited or Default alarm profiles.

Note A previously created alarm profile cannot be deleted unless it has been stored on the node. If the profile is visible on the Alarm Profiles tab but is not listed in the Select Node/Profile Combinations to Delete dialog box, continue with Step 9.

Step 6 Click the node name(s) in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 7 Click the profile name(s) you want to delete in the Profile Names list.

Step 8 Click **OK**.

Click **Yes** in the Delete Alarm Profile dialog box.

Note If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.

Step 9 To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a node and profile combination is selected but does not exist, a warning appears: "One or more of the profile(s) selected do not exist on one or more of the node(s) selected." For example, if node A has only profile 1 stored and the user tries to delete both profile 1 and profile 2 from node A, this warning appears. However, the operation still removes profile 1 from node A.

Note The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

Step 10 Return to your originating procedure (NTP).

NTP-A168 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	This procedure starts, changes, or stops alarm filtering for one or more severities in the Alarms, Conditions, and History windows in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to enable alarm severity filtering. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-A225 Enable Alarm Filtering" task on page 9-29. This task enables alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms, conditions, or events.

Step 3 As necessary, complete the "DLP-A521 Modify Alarm, Condition, and History Filtering Parameters" task on page 9-30 to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-A227 Disable Alarm Filtering" task on page 9-32 to disable alarm profile filtering for all network nodes.

Stop. You have completed this procedure.

DLP-A225 Enable Alarm Filtering

Purpose	This task enables alarm filtering for alarms, conditions, or event history in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.

If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.

Step 3 If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.

Step 4 If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.

Step 5 Return to your originating procedure (NTP).

DLP-A521 Modify Alarm, Condition, and History Filtering Parameters

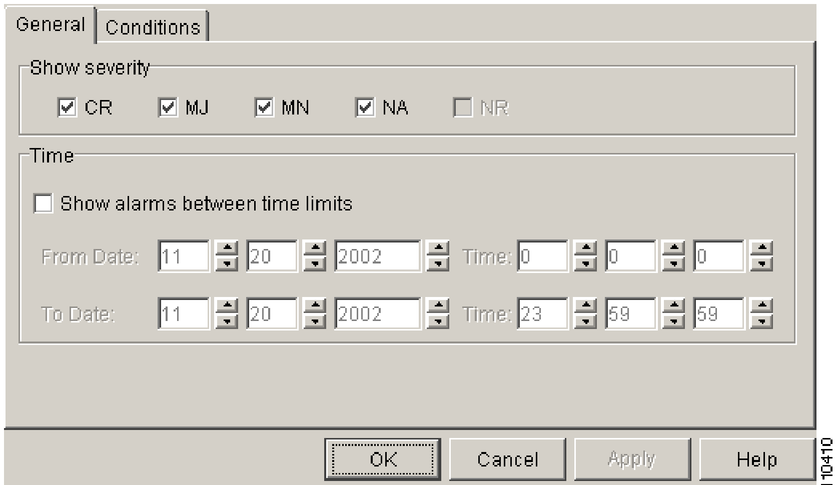
Purpose	This task changes alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 9-29
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card view, click the **Alarms** tab, Conditions tab, or History tab.

Step 2 Click the **Filter** button at the lower-left of the bottom toolbar.

The filter dialog box appears, displaying the General tab. Figure 9-13 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

Figure 9-13 Alarm Filter Dialog Box General Tab



In the General tab Show Severity box, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to Step 3. To change the time period filter for the alarms go to Step 4.

Step 3 In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA)] you want to be reported at the network level. Leave severity check boxes deselected (unchecked) to prevent those severities from appearing.

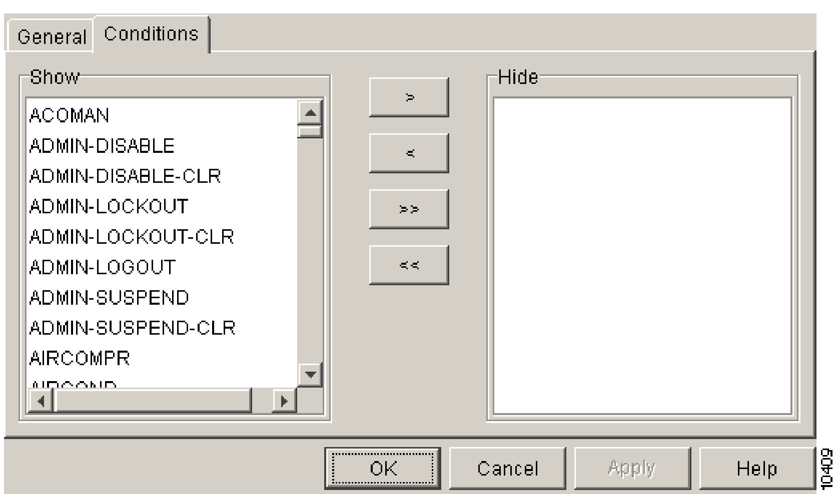
When alarm filtering is disabled, all alarms show.

Step 4 In the Time area, click the **Show alarms between time limits** check box to enable it. Click the up and down arrows in the From Date, To Date, and Time fields to modify what period of alarms are shown.

To modify filter parameters for conditions, continue with Step 5. If you do not need to modify them, continue with Step 6.

Step 5 Click the filter dialog box **Conditions** tab (Figure 9-14).

Figure 9-14 Alarm Filter Dialog Box Conditions Tab



When filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the > button.
- To move conditions individually from the Hide list to the Show list, click the < button.
- To move conditions collectively from the Show list to the Hide list, click the >> button.
- To move conditions collectively from the Hide list to the Show list, click the << button.

Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-A225 Enable Alarm Filtering" task on page 9-29), and are not enforced when alarm filtering is disabled (see the "DLP-A227 Disable Alarm Filtering" task on page 9-32).

Step 7 Return to your originating procedure (NTP).

DLP-A227 Disable Alarm Filtering

Purpose	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering, page 9-29 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is indented and disabled if the tool is raised (not selected).

Step 3 If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and click the Filter tool.

Step 4 If you want alarm filtering disabled when you view alarm history, click the **History** tab and click the Filter tool.

Step 5 Return to your originating procedure (NTP).

NTP-A72 Suppress Alarms or Discontinue Alarm Suppression

Purpose	This procedure prevents alarms from being reported for a port, card, or node in circumstances when an alarm or condition is known to exist but you do not want to include it in the display. This procedure also resumes normal alarm reporting by discontinuing the suppression.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A522 Suppress Alarm Reporting" task on page 9-33 to enable the node to send autonomous messages that clear specific raised alarms and cause suppressed alarms to appear in the Conditions window.

Note Suppressing one or more alarms prevents them from appearing in Alarm or History windows or in any other clients. The suppress command causes CTC to display them in the Conditions window with their severity, their severity color code, and service-affecting status.

Step 3 Complete the "DLP-A523 Discontinue Alarm Suppression" task on page 9-35 to discontinue alarm suppression and resume normal alarm reporting.

Stop. You have completed this procedure.

DLP-A522 Suppress Alarm Reporting

Purpose	This task suppresses the reporting of ONS 15454 alarms at the node, card, or port level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Caution If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

Note Alarm suppression at the node level does not supersede alarm suppression at the card or port level. Suppression can exist independently for all three entities, and each entity will raise separate alarms suppressed by the user command (AS-CMD) alarm.

Step 1 If you are in node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 2 To suppress alarms for the entire node:

a. Check the **Suppress Alarms** check box.

b. Click **Apply**.

All raised alarms for the node will change color to white in the Alarms window and their status will change to cleared. After suppressing alarms, clicking **Synchronize** in the Alarms window will remove cleared alarms from the window. However, an AS-CMD alarm will show in node or card view to indicate that node-level alarms were suppressed; this alarm will show System in the Object column.

Note The only way to suppress BITS, power source, or system alarms is to suppress alarms for the entire node. These cannot be suppressed separately, but the shelf backplane can be.

Step 3 To suppress alarms for individual cards:

a. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).

b. Check the **Suppress Alarms column** check box on that row (Figure 9-11 on page 9-26).

Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for an OC-48 card in Slot 16, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number. For example, if you suppressed alarms for a Slot 16 OC-48 card, the AS-CMD object will be "SLOT-16."

Click **Apply**.

Step 4 To suppress alarms for individual card ports double-click the card in node view.

Step 5 Depending on which card ports you want to suppress alarm reporting on, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SONET ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.

- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 6 Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 9-10 on page 9-25).

Step 7 Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the entire card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 16 OC-48 card, the alarm object will show “FAC-16-1.”

Step 8 Return to your originating procedure (NTP).

DLP-A523 Discontinue Alarm Suppression

Purpose	This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A522 Suppress Alarm Reporting, page 9-33 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Caution If multiple CTC sessions are open, discontinuing suppression in one session will discontinue suppression in all other open sessions.

Step 1 To discontinue alarm suppression for the entire node:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tab.

b. Uncheck the **Suppress Alarms** check box.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the System object will be cleared in all views.

Step 2 To discontinue alarm suppression for individual cards:

a. In the node view, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

b. Locate the card that was suppressed in the slot list.

c. Uncheck the Suppress Alarms column check box for that slot.

d. Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the slot object (for example, SLOT-16) will be cleared in all views.

Step 3 To discontinue alarm suppression for ports, click the following tabs:

- If the card is an E-Series Ethernet, G-Series Ethernet, MXP, TXP, TXPP, OC-N, or electrical (DS-1, DS-1N, DS-3, DS-3E, DS-3I, DS-3I-N, DS-3N, DS-3NE, or EC-1) card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an ML-Series Ethernet (traffic) card, click the **Provisioning > Ether Alarming > Alarm Profiles** tabs or the **Provisioning > POS Alarming > Alarm Profiles** tabs, depending on whether you want to apply the profile to the front physical ports ("Ether alarming") or packet over SONET ("POS alarming"). For more information about ML-Series card ports and service, see the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- If the card is an OSC-CSM card, click the **Provisioning > OC3 Line > Alarm Profiles > Alarm Profiles** tabs or **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 32MUX-O or 32DMX-O card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is a 4MD card, click the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an OPT-PRE or OPT-BST card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Opt. Ampli. Line > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1C, AD-2C, or AD-4C card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Chn > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an AD-1B or AD-4B card, click the **Provisioning > Optical Line > Alarm Profiles > Alarm Profiles** tabs or the **Provisioning > Optical Band > Alarm Profiles > Alarm Profiles** tabs.
- If the card is an FCMR card, click the **Provisioning > Alarm Profiles > Alarm Profiles** tabs.

Step 4 Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.

Step 5 Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD alarm with the port object (for example, FAC-16-1) will be cleared in all views.

Step 6 Return to your originating procedure (NTP).

NTP-A32 Provision External Alarms and Controls on the Alarm Interface Controller

Purpose	This procedure creates external (environmental) alarms and external controls for the Alarm Interface Controller (AIC) card.
Tools/Equipment	An AIC card must be installed in Slot 9.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For information about the AIC external alarms and controls, virtual wire, and orderwire, refer to the *Cisco ONS 15454 Reference Manual*.

Step 1 Verify the backplane wiring. See the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-37 for information about the ONS 15454 backplane pins.

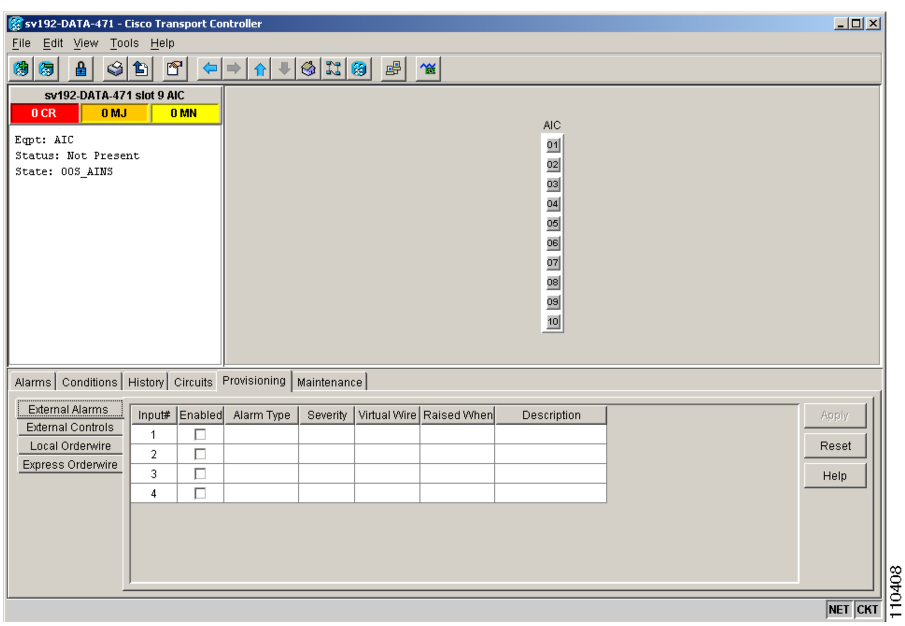
a. For external alarms, verify that the external-device relays are wired to the ENVIR ALARMS IN backplane pins.

b. For external controls, verify that the external relays are wired to the ENVIR ALARMS OUT backplane pins.

Step 2 In the node view, double-click the AIC card on the shelf graphic. The card view appears.

Step 3 If you are provisioning external alarms, click the **Provisioning > External Alarms** tab (Figure 9-15). If you are not provisioning external alarms, skip Steps 4 through 6 and go to Step 7.

Figure 9-15 AIC Card External Alarms



Step 4 Complete the following fields for each external device wired to the ONS 15454 backplane:

- Enabled—Check the check box to activate the fields for the alarm input number.
- Alarm Type—Choose an alarm type from the drop-down list.
- Severity—Click a severity in the drop-down list.

  The severity you choose determines the external alarm's severity in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.
- Virtual Wire—Choose the virtual wire number in the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the AIC virtual wire, see the *Cisco ONS 15454 Reference Manual*.
- Raised When—From the drop-down list, choose the contact condition (open or closed) that triggers the alarm.
- Description—A default description is provided; enter a different description if needed.

Step 5 To provision up to four virtual wire inputs for external devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 If you are provisioning external control outputs for external devices, click the **External Controls** subtab.

Step 8 Complete the following options for each external control wired to the ONS 15454 backplane:

- Enabled—Check this check box to activate the fields for the alarm input number.
- Control Type—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- Trigger Type—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- Description—Enter a description.

Step 9 To provision additional external controls, complete Steps 7 and 8 for each additional device.

Step 10 Click **Apply**.

Note If you provision an external alarm to raise upon an open contact before you physically connect to the ONS equipment, the alarm will raise until you do create the physical connection.

Note When you provision an external alarm, the alarm object is ENV-IN-nn. The variable nn refers to the external alarm's number, regardless of the name you assign.

Note Environmental alarms that you create (and name) should be recorded locally for the NE. Both the Alarm name and resolution are node-specific.

Stop. You have completed this procedure.

NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International

Purpose	This procedure creates external (environmental) alarms and external controls for the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The AIC-I card alarm provides direct alarm contacts (external alarm inputs and external control outputs) routed through the backplane to wire-wrap pins accessible from the back of the shelf. If you install an Alarm Expansion Panel (AEP), the AIC-I alarm contacts cannot be used. Only the alarm expansion panel (AEP) alarm contacts can be used. For further information about the AEP, see "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-34 and the "NTP-A120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-44.

Note For information about the AIC-I alarms, controls, and virtual wire, refer to the *Cisco ONS 15454 Reference Manual*.

Step 1 Verify the backplane wiring. If you are using the AEP, see the "NTP-A119 Install the Alarm Expansion Panel" procedure on page 1-34. Otherwise, see the "NTP-A8 Attach Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-37 for information about the ONS 15454 backplane pins.

a. For external alarms, verify that the external device relays are wired to the ENVIR ALARMS IN backplane pins.

b. For external controls, verify that the external device relays are wired to the ENVIR ALARMS OUT backplane pins.

Step 2 In the node view, double-click the AIC-I card on the shelf graphic. The card view appears.

Step 3 Click the **Provisioning > Card** tabs.

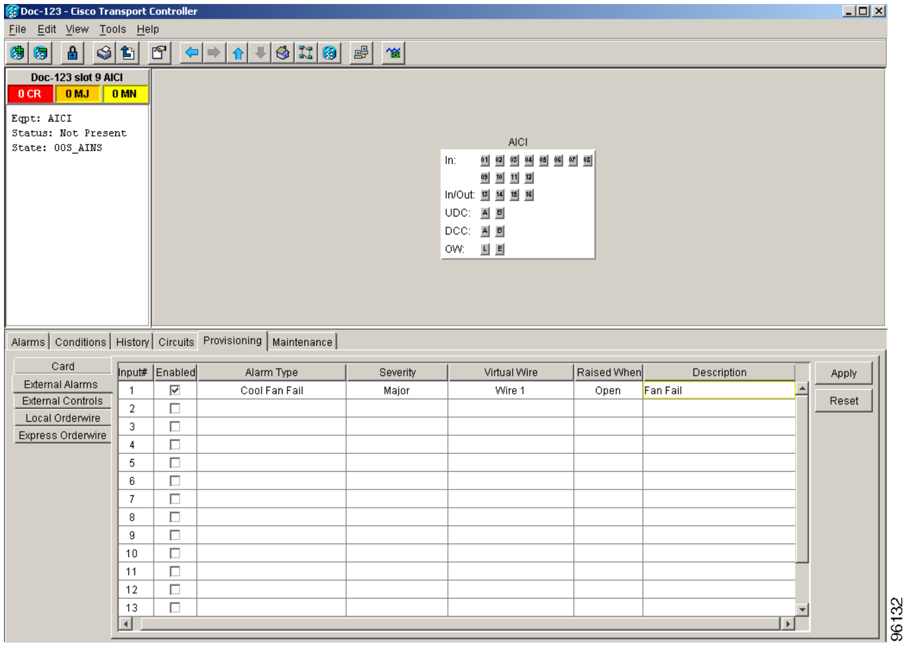
Step 4 In the Alarm Contacts area, click the Add Extension radio button if you are using the AEP. Clicking this option will choose the External Alarm input/output type and the AEP extension type; it will give you access to 16 external alarm contacts.

Step 5 If you did not click Add Extension, in the Input/Output area, choose either External Alarm or External Control. (External Alarm will limit your input/output options as explained in Step 4.) Choosing External Control will enable both external alarms and external controls. This will convert four of the external alarm contacts to external controls, leaving 12 available external control contacts. The extension type for both options is AEP.

Step 6 Click **Apply**.

Step 7 If you are provisioning external alarms, click the **External Alarms** tab (Figure 9-16). If you are not provisioning external alarms, skip Steps 8 through 10 and go to Step 11.

Figure 9-16 Provisioning External Alarms On The AIC-I Card



Step 8 For external alarms, complete the following fields:

- Enabled—Check the check box to activate the fields for the alarm input number.
- Alarm Type—Choose an alarm type from the drop-down list.
- Severity—Click a severity from the drop-down list.

  The severity determines the alarm's severity in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.
- Virtual Wire—Choose the virtual wire number from the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the AIC-I virtual wire, see the *Cisco ONS 15454 Reference Manual*.
- Raised When—From the drop-down, choose the contact condition (open or closed) that triggers the alarm.
- Description—A default description is provided; enter a different description if needed.

Step 9 To provision additional devices, complete Step 8 for each additional device.

Step 10 Click **Apply**.

Step 11 For external controls, click the **External Controls** tab and complete the following fields for each control wired to the ONS 15454 backplane:

- Enabled—Check this check box to activate the fields for the alarm input number.
- Control Type—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- Trigger Type—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- Description—Enter a description.

Step 12 To provision additional external controls, complete Step 11 for each device.

Step 13 Click **Apply**.

> **Note** When you provision an external alarm, the alarm object is ENV-IN-nn. The variable nn refers to the external alarm's number, regardless of the name you assign.

> **Note** Environmental alarms that you create (and name) should be recorded locally for the NE. Both the Alarm name and resolution are node-specific.

Stop. You have completed this procedure.

CHAPTER 10

Monitor Performance

This chapter explains how to enable and view performance monitoring statistics for the Cisco ONS 15454. Performance monitoring (PM) parameters are used by service providers to gather, store, and set thresholds and report performance data for early detection of problems. For more PM information, details, and definitions refer to the *Cisco ONS 15454 Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A253 Change the PM Display, page 10-2—Complete as needed to change the displayed PM counts.
2. NTP-A195 Monitor Electrical Performance, page 10-10—Complete as needed to monitor electrical performance.
3. NTP-A198 Monitor Ethernet Performance, page 10-12—Complete as needed to monitor Ethernet performance.
4. NTP-A279 Create or Delete Ethernet RMON Thresholds, page 10-20—Complete as needed to monitor Ethernet performance.
5. NTP-A250 Monitor OC-N Performance, page 10-26—Complete as needed to monitor optical (OC-*N)* performance.
6. NTP-A251 Monitor Multirate Transport Performance, page 10-32—Complete as needed to monitor multirate transport performance.
7. NTP-A252 Monitor DWDM Performance, page 10-40—Complete as needed to monitor DWDM performance.
8. NTP-A285 Monitor FC_MR-4 Performance, page 10-48—Complete as needed to monitor FC_MR-4 performance.
9. NTP-A289 Create or Delete FC_MR-4 RMON Thresholds, page 10-51—Complete as needed to monitor FC_MR-4 performance.

Note For additional information regarding PM parameters, refer to the Digital transmission surveillance section in Telcordia's GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE documents, and in the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

NTP-A253 Change the PM Display

Purpose	This procedure enables you to change the display of PM counts by selecting drop-down menu or radio button options in the Performance window.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2

Step 2 In node view, double-click the electrical, Ethernet, optical (OC-N), multirate transport, or DWDM cards where you want to view PM counts. The card view appears.

Step 3 As needed, use the following tasks to change the display of PM counts:

- DLP-A124 Refresh PM Counts at 15-Minute Intervals, page 10-3
- DLP-A125 Refresh PM Counts at One-Day Intervals, page 10-3
- DLP-A347 Refresh E-Series and G-Series Ethernet PM Counts, page 10-4
- DLP-A126 View Near-End PM Counts, page 10-5
- DLP-A127 View Far-End PM Counts, page 10-6
- DLP-A348 Monitor PM Counts for a Selected Signal, page 10-6
- DLP-A129 Reset Current PM Counts, page 10-8
- DLP-A349 Clear Selected PM Counts, page 10-8
- DLP-A260 Set Auto-Refresh Interval for Displayed PM Counts, page 10-9
- DLP-A261 Refresh PM Counts for a Different Port, page 10-10

Stop. You have completed this procedure.

DLP-A124 Refresh PM Counts at 15-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** radio button.

Step 4 Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A125 Refresh PM Counts at One-Day Intervals

Purpose	This task changes the window view to display PM parameters in 1-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** radio button.

Step 4 Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 1-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 1-day interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

> **Note** If a complete count over a 1-day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A347 Refresh E-Series and G-Series Ethernet PM Counts

Purpose	This task changes the window view to display E-Series and G-Series Ethernet PM parameters intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > History** tabs.

Step 3 From the Interval drop-down menu click one of the following:

- 1 min
- 15 min
- 1 hour
- 1 day

Step 4 Click **Refresh**. Performance monitoring appears in the interval selected synchronized with the time of day.

Step 5 View the Prev column to find PM counts for the latest selected interval.

Each monitored performance parameter has corresponding threshold values for the latest time period. If the value of the counter exceeds the threshold value for a particular selected interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous intervals.

> **Note** If a complete count over the selected interval is not possible, the value appears with a yellow background. For example, if you selected the 1-day interval, an incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-A126 View Near-End PM Counts

Purpose	This task enables you to view near-end PM counts for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** radio button.

Step 4 Click **Refresh**. All PM parameters occurring for the selected card on the incoming signal appear. For PM parameter definitions refer to the *Cisco ONS 15454 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-A127 View Far-End PM Counts

Purpose	This task enables you to view far-end PM parameters for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** radio button.

Step 4 Click **Refresh**. All PM parameters recorded by the far-end node for the selected card on the outgoing signal appear. For PM parameter definitions refer to the *Cisco ONS 15454 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-A348 Monitor PM Counts for a Selected Signal

Purpose	This task enables you to view near-end or far-end PM counts for a specific signal (STS*n*), path (VT*n*) and port (DS*n*) on a selected card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Note Different port and signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM card lists DS3, DS1, VT path, and STS path PM parameters as signal-types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

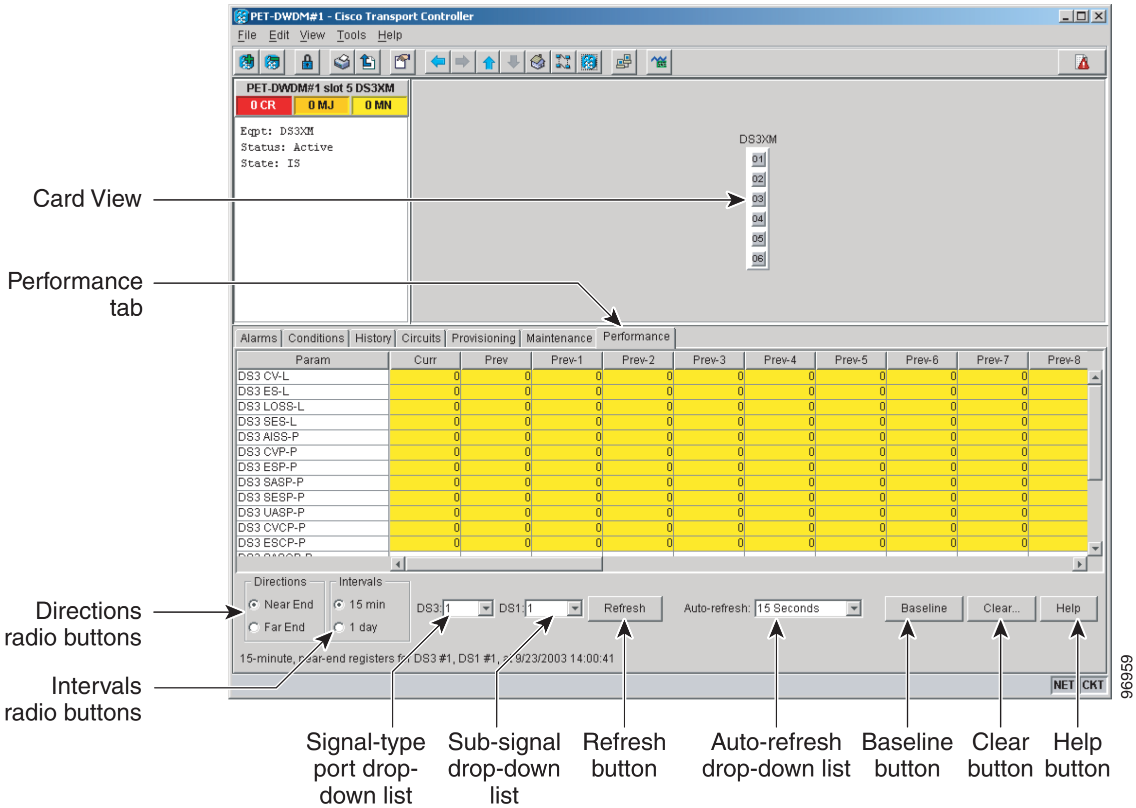
Step 3 In the signal type drop-down menus, click the following options as appropriate:

- DS: *n* or Port: *n* (card port number)

- VT: *n* (VT path number)
- STS: *n* (STS number within the VT path)

Figure 10-1 shows the Port and Signal-type menus on the Performance window for a DS3XM-6 card.

Figure 10-1 Signal-Type Menus for a DS3XM-6 Card



Step 4 Click **Refresh**. All PM counts recorded by the near-end or far-end node for the specified outgoing signal type on the selected card and port appear. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

DLP-A129 Reset Current PM Counts

Purpose	This task clears the current PM count, but it does not clear the cumulative PM count. This task allows you to see how quickly PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Baseline**.

Note The Baseline button clears the PM counts displayed in the current time interval but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance window.

Step 4 View the current statistics columns to observe changes to PM counts for the current time interval.

Step 5 Return to your originating procedure (NTP).

DLP-A349 Clear Selected PM Counts

Purpose	This task uses the Clear button to clear specified PM counts depending on the option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes. After pressing this button the current bin is marked invalid. Also note that the UAS state is not cleared if you were counting UAS; therefore, this count could be unreliable when UAS is no longer counting.

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Clear**.

Step 4 From the Clear Statistics menu, choose one of three options:

- Displayed statistics: Clearing displayed statistics erases from the card and the window all PM counts associated with the current combination of statistics on the selected port. This means the selected time interval, direction, and signal type counts are erased from the card and the window.
- All statistics for port x: Clearing all statistics for port x erases from the card and the window all PM counts associated with all combinations of the statistics on the selected port. This means all time intervals, directions, and signal type counts are erased from the card and the window.
- All statistics for card: Clearing all statistics for card erases from the card and the window all PM counts for all ports.

Step 5 From the Clear Statistics menu, choose **OK** to clear the selected statistics.

Step 6 Verify that the selected PM counts have been cleared.

Step 7 Return to your originating procedure (NTP).

DLP-A260 Set Auto-Refresh Interval for Displayed PM Counts

Purpose	This task changes the window auto-refresh intervals for updating the displayed PM counts.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 From the Auto-refresh drop-down menu, choose one of six options:

- None: This option disables the auto-refresh feature.
- 15 Seconds: This option sets the window auto-refresh to 15-second time intervals.
- 30 Seconds: This option sets the window auto-refresh to 30-second time intervals.
- 1 Minute: This option sets the window auto-refresh to 1-minute time intervals.
- 3 Minutes: This option sets the window auto-refresh to 3-minute time intervals.
- 5 Minutes: This option sets the window auto-refresh to 5-minute time intervals.

Step 4 Click **Refresh**. The PM counts for the newly-selected auto-refresh time interval appear.

Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the PM counts that appear are not updated unless you click Refresh.

Step 5 Return to your originating procedure (NTP).

DLP-A261 Refresh PM Counts for a Different Port

Purpose	This task changes the window view to display PM counts for another port on a multiport card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 In the Port drop-down menu, choose a port.

Step 4 Click **Refresh**. The PM counts for the newly-selected port appear.

Step 5 Return to your originating procedure (NTP).

NTP-A195 Monitor Electrical Performance

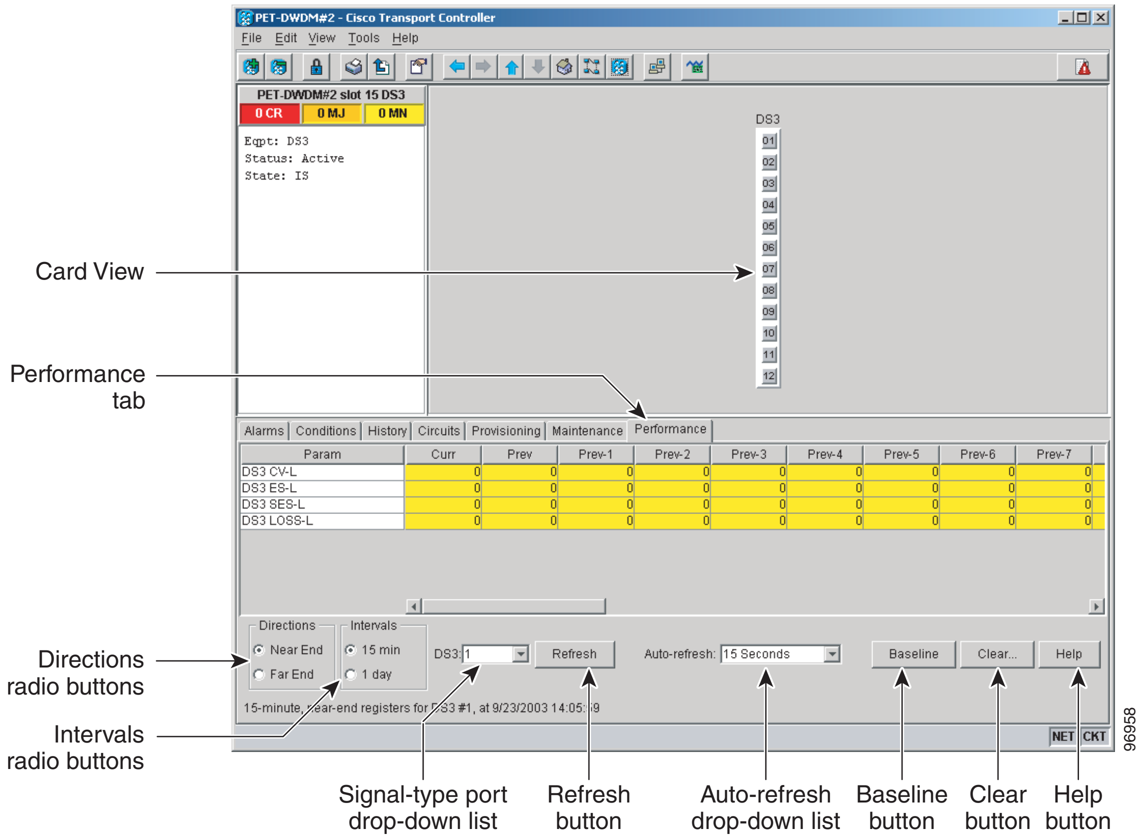
Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on an electrical card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the electrical card where you want to view PM counts. The card view appears.

Step 3 Click the **Performance** tab (Figure 10-2).

Figure 10-2 Viewing Electrical Card Performance Monitoring Information



Step 4 In the signal type drop-down menus, click one of the following options:

- DS*n* (card port)
- VT*n* (VT path)
- STS*n* (STS within the VT path)

Step 5 Click **Refresh**.

Step 6 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Stop. You have completed this procedure.

NTP-A198 Monitor Ethernet Performance

Purpose	This procedure enables you to view node transmit and receive performance during selected time intervals on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A256 View Ethernet Statistics PM Parameters" task on page 10-12.

Step 3 Complete the "DLP-A257 View Ethernet Utilization PM Parameters" task on page 10-14.

Step 4 Complete the "DLP-A258 View Ethernet History PM Parameters" task on page 10-15.

Step 5 Complete the "DLP-A320 View ML-Series Ether Ports PM Parameters" task on page 10-17.

Step 6 Complete the "DLP-A321 View ML-Series POS Ports PM Parameters" task on page 10-18.

Stop. You have completed this procedure.

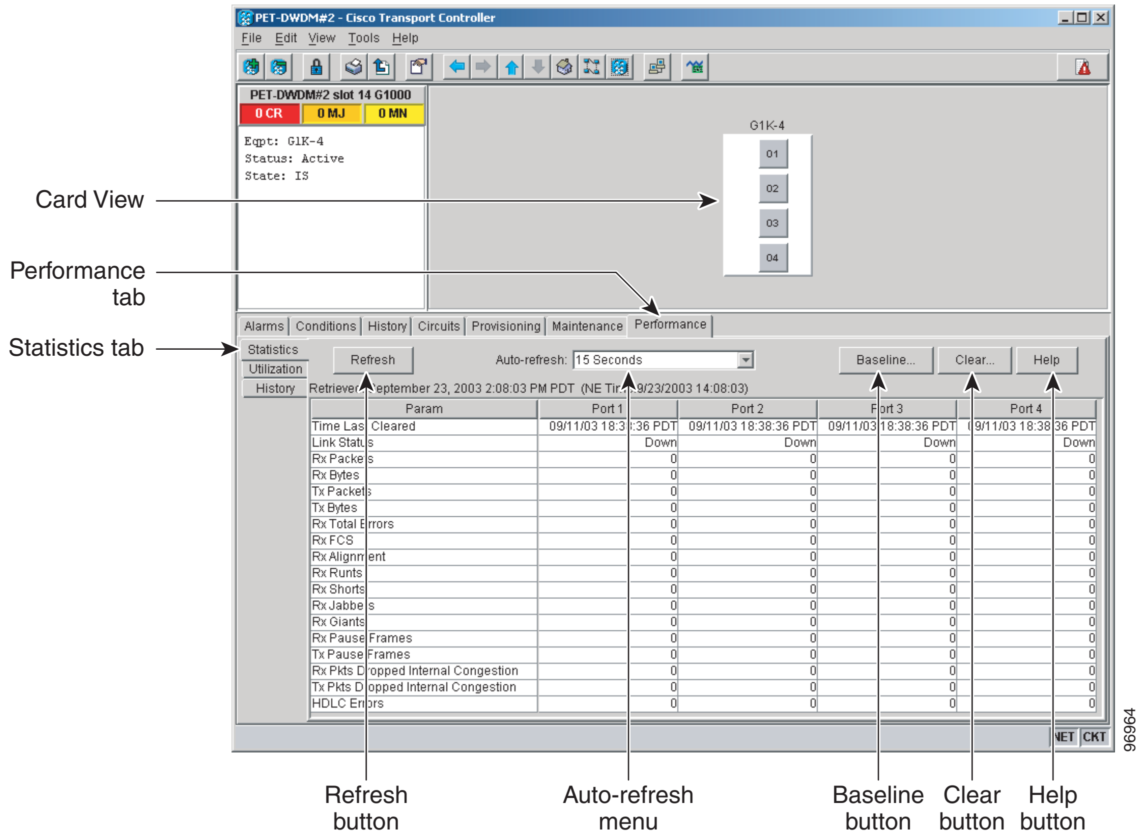
DLP-A256 View Ethernet Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Statistics** tabs (Figure 10-3).

Figure 10-3 G-Series Statistics on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

> **Note** To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Step 5 Return to your originating procedure (NTP).

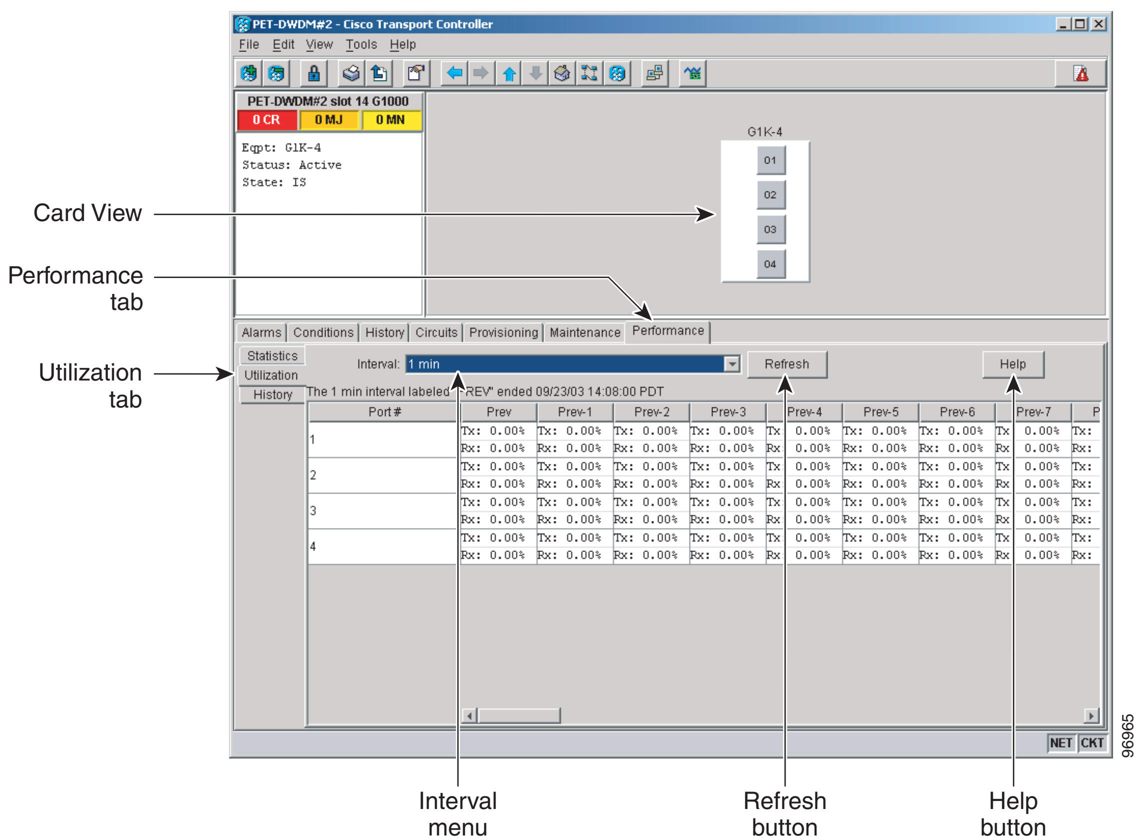
DLP-A257 View Ethernet Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Utilization** tabs (Figure 10-4).

Figure 10-4 G-Series Utilization on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column to find the port you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Step 6 Return to your originating procedure (NTP).

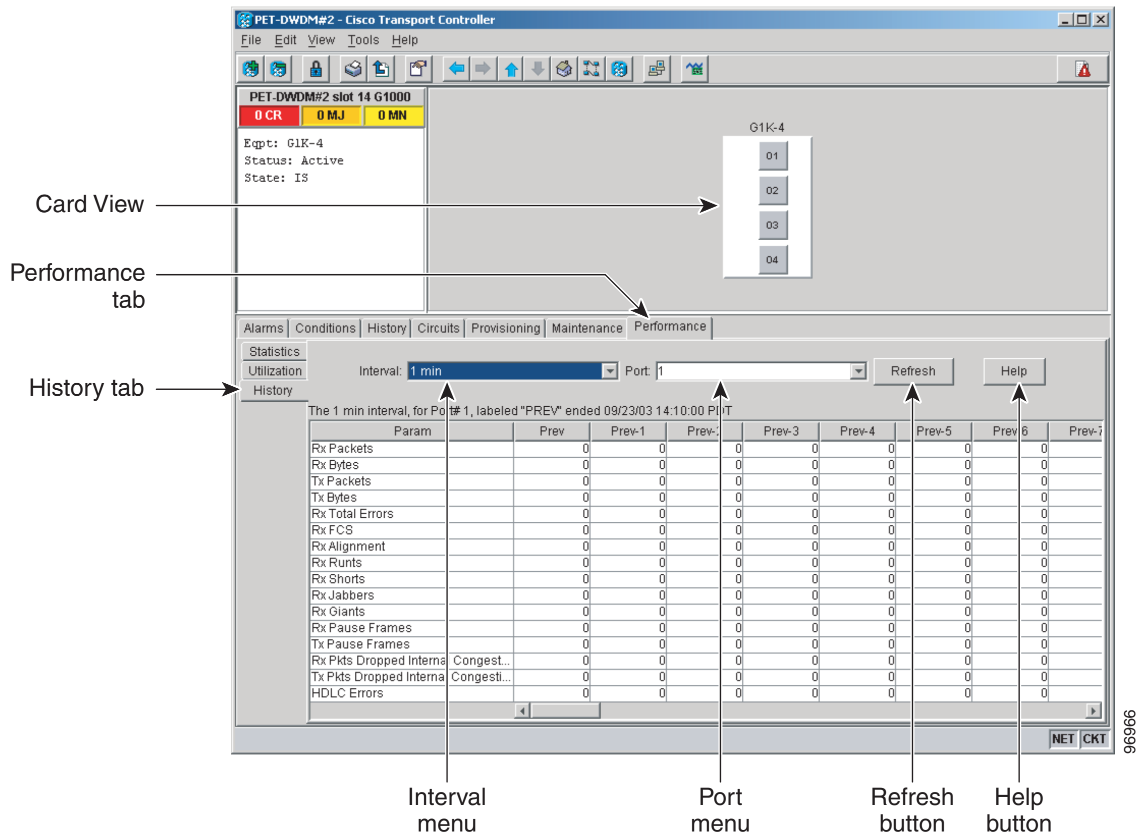
DLP-A258 View Ethernet History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **History** tabs (Figure 10-5).

Figure 10-5 Ethernet History on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Step 5 Return to your originating procedure (NTP).

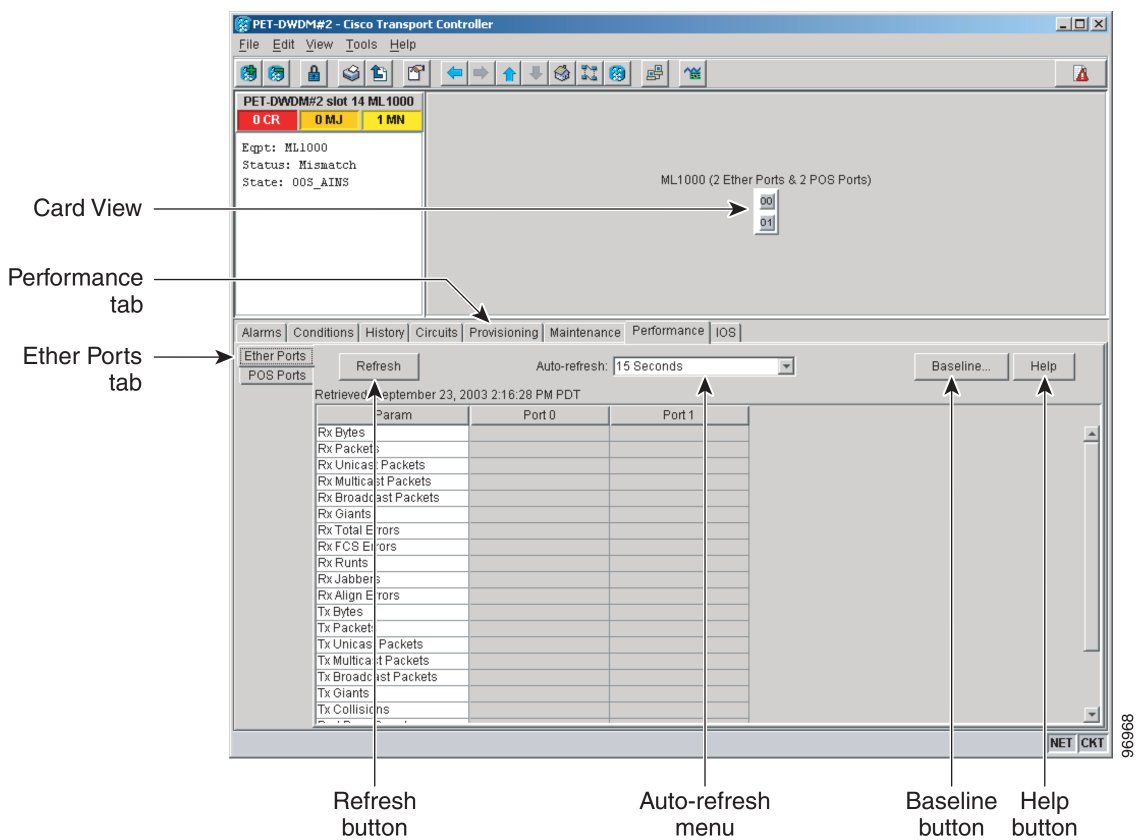
DLP-A320 View ML-Series Ether Ports PM Parameters

Purpose	This task enables you to view ML-Series Ethernet port PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Ether Ports** tabs (Figure 10-6).

Figure 10-6 Ether Ports on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Step 5 Return to your originating procedure (NTP).

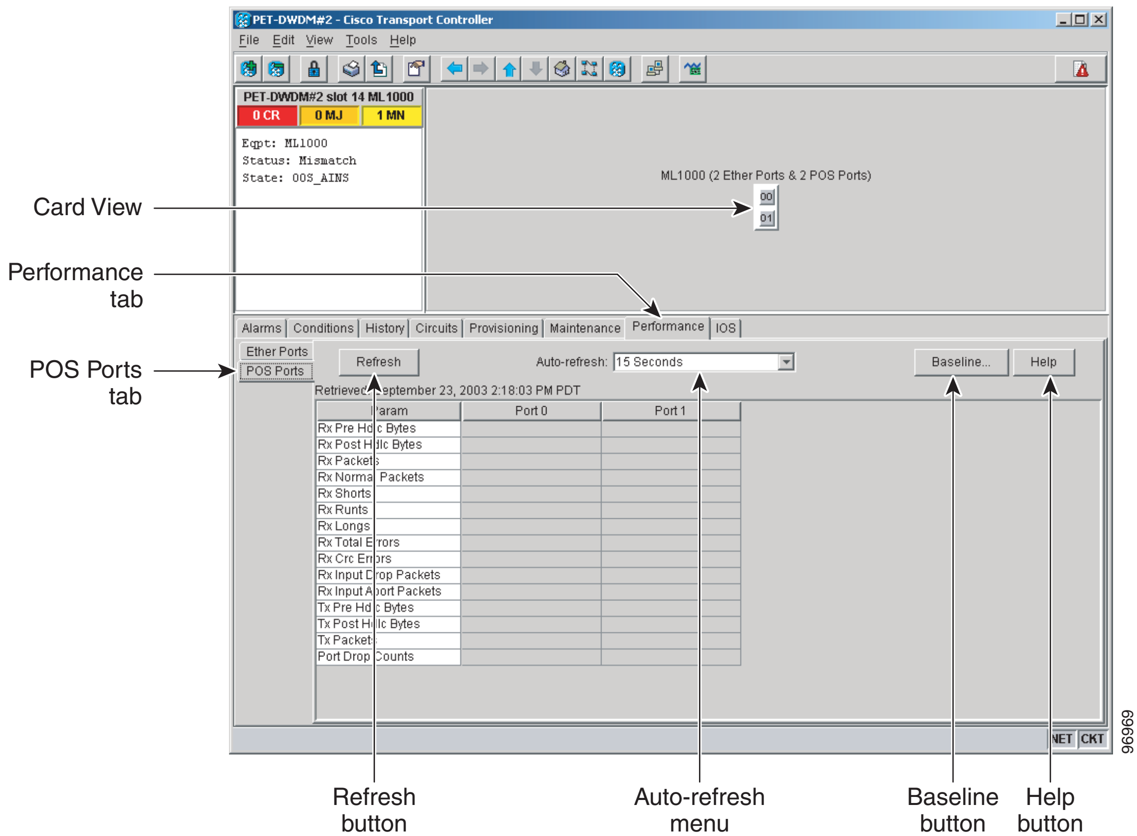
DLP-A321 View ML-Series POS Ports PM Parameters

Purpose	This task enables you to view Packet Over SONET (POS) port PM counts at selected time intervals on an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **POS Ports** tabs (Figure 10-7).

Figure 10-7 POS Ports on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions refer to the *Cisco ONS 15454 Reference Manual*.

Note To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Step 5 Return to your originating procedure (NTP).

DLP-A259 Refresh Ethernet PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the Ethernet card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Utilization** tab or the **History** tab.

Step 4 From the Interval drop-down menu, choose one of four options:

- 1 min: This option appears the specified PM counts in one-minute time intervals.
- 15 min: This option appears the specified PM counts in 15-minute time intervals.
- 1 hour: This option appears the specified PM counts in one-hour time intervals.
- 1 day: This option appears the specified PM counts in one-day (24 hours) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the selected time interval.

Step 6 Return to your originating procedure (NTP).

NTP-A279 Create or Delete Ethernet RMON Thresholds

Purpose	This procedure creates or deletes Ethernet remote monitoring (RMON) thresholds for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series card uses the Cisco IOS CLI for managing RMON.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-A533 Create Ethernet RMON Alarm Thresholds, page 10-21
- DLP-A529 Delete Ethernet RMON Alarm Thresholds, page 10-26

Stop. You have completed this procedure.

DLP-A533 Create Ethernet RMON Alarm Thresholds

Purpose	This procedure sets up remote monitoring (RMON) to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series card uses the Cisco IOS CLI for managing RMON.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to set up RMON. If you are already logged in, continue with Step 2.

Step 2 Double-click the Ethernet card where you want to create the RMON alarm thresholds.

Step 3 In card view, click the **Provisioning > Ether Thresholds** tabs.

Step 4 Click **Create**.

The Create Ether Threshold dialog box appears (Figure 10-8).

Figure 10-8 Creating RMON Thresholds

Step 5 From the Slot menu, choose the appropriate Ethernet card.

Step 6 From the Port drop-down menu, choose the applicable port on the Ethernet card you selected.

Step 7 From the Variable drop-down menu, choose the variable. See Table 10-1 for a list of the Ethernet threshold variables available in this field.

Step 8 From the Alarm Type drop-down menu, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 9 From the Sample Type drop-down menu, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 10 Type in an appropriate number of seconds for the Sample Period.

Step 11 Type in the appropriate number of occurrences for the Rising Threshold.

Note For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 12 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15 minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 13 Click **OK** to complete the procedure.

Table 10-1 Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts (G-Series only)	Number of multicast frames received error free
ifInBroadcastPkts (G-Series only)	The number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a broadcast address at this sublayer
ifInDiscards (G-Series only)	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts (G-Series only)	Number of multicast frames transmitted error free

Table 10-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
ifOutBroadcastPkts (G-Series only)	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
ifOutDiscards (G-Series only)	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, the length is not an integral number of octets and the frame cannot pass the frame check sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames (not supported by E-Series or G-Series)	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrames (not supported by E-Series or G-Series)	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions (not supported by E-Series or G-Series)	Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollisions (not supported by E-Series or G-Series)	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollisions (not supported by E-Series or G-Series)	Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors (G-Series only)	The number of transmission errors on a particular interface that are not otherwise counted
dot3StatsSQETestErrors (G-Series only)	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.

Table 10-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsCollisions	An estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BASE-T. Section 14.2.1.4 (10BASE-T) of the IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
etherStatsCollisionFrames	An estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment. Probe location plays a much smaller role when considering 10BASE-T. Section 14.2.1.4 (10BASE-T) of the IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. An RMON probe inside a repeater should report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.

Table 10-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast.
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length
receivePauseFrames (G series only)	The number of received IEEE 802.x pause frames
transmitPauseFrames (G series only)	The number of transmitted IEEE 802.x pause frames
receivePktsDroppedInternalCongestion (G series only)	The number of received framed dropped due to frame buffer overflow as well as other reasons
transmitPktsDroppedInternalCongestion (G series only)	The number of frames dropped in the transmit direction due to frame buffer overflow as well as other reasons
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets

Stop. **You have completed this procedure**.

DLP-A529 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A533 Create Ethernet RMON Alarm Thresholds, page 10-21 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15454 ML-Series card uses the Cisco IOS CLI for managing RMON.

Step 1 Double-click the Ethernet card where you want to delete the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning** > **Ether Thresholds** tabs.

Step 3 Click the RMON alarm threshold you want to delete.

Step 4 Click **Delete**. The Delete Threshold dialog box opens.

Step 5 Click **Yes** to delete that threshold.

Step 6 Return to your originating procedure (NTP).

NTP-A250 Monitor OC-N Performance

Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on an OC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2

Step 2 Complete the "DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring" task on page 10-27 as needed to enable or disable clock synchronization monitoring.

Step 3 Complete the "DLP-A122 Enable/Disable Intermediate Path Performance Monitoring" task on page 10-29 as needed to enable or disable monitoring of STS traffic through intermediate nodes.

Step 4 Complete the "DLP-A507 View OC-N PM Parameters" task on page 10-31.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Stop. You have completed this procedure.

DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring

Purpose	This task enables or disables pointer justification counts, which provide a way to align the phase variations in STS payloads and to monitor the clock synchronization between nodes. A consistently large pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card you want to monitor. The card view appears.

See Table 10-2 for a list of LTE cards.

Table 10-2 OC-N Cards that Terminate the Line, Called LTEs

Line Terminating Equipment
EC1-12
OC3 IR 4/STM1 SH 1310
OC3 IR4/STM1 SH 1310-8
OC12 LR/STM4 LH 1310
OC12 IR/STM4 SH 1310
OC12 IR/STM4 SH 1310-4
OC12 LR/STM4 LH 1550
OC48 LR 1550
OC48 IR 1310
OC48 LR/STM16 LH AS 1550
OC48 IR/STM16 SH AS 1310
OC48 ELR 200 GHz

Table 10-2 OC-N Cards that Terminate the Line, Called LTEs (continued)

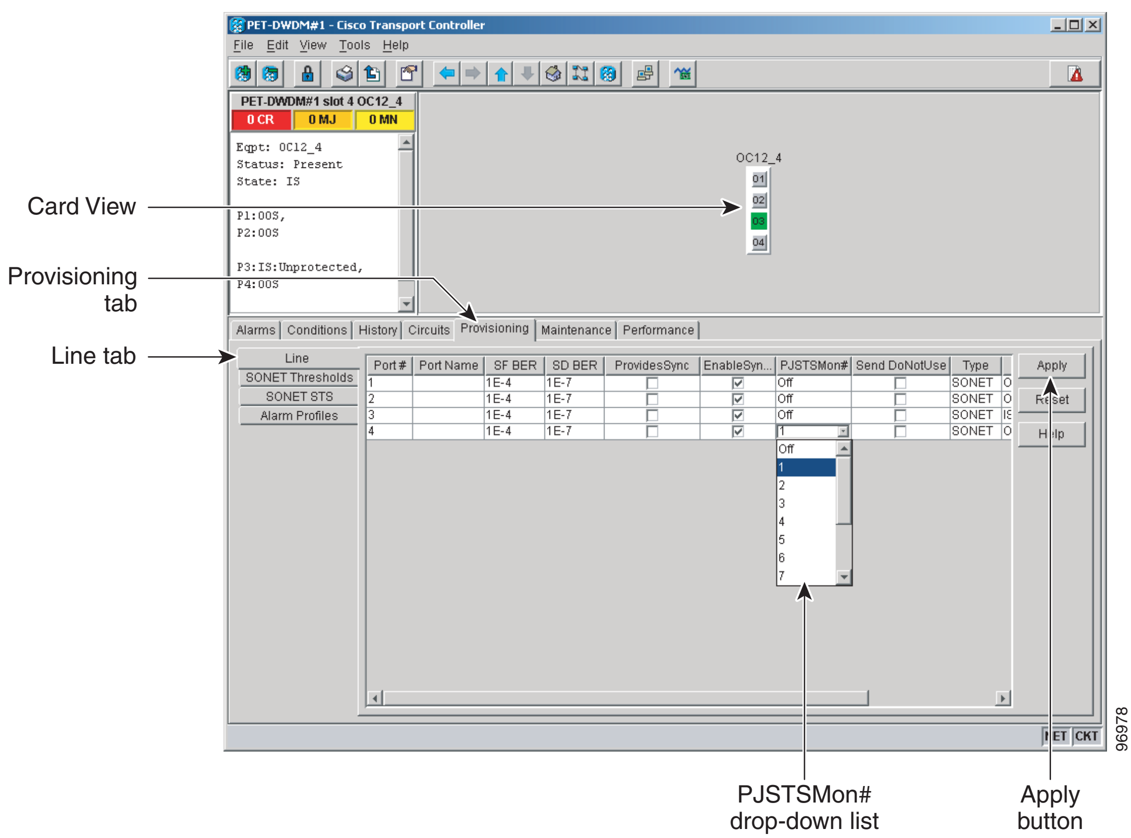
Line Terminating Equipment
OC48 ELR/STM16 EH 100 GHz
OC192 SR/STM64 IO 1310
OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550
OC192 ELR/STM64 LH ITU 15xx.xx

Step 2 Click the **Provisioning > Line** tabs.

Step 3 From the PJSTSMon# drop-down menu, make a selection based on the following rules (Figure 10-9):

- Off means pointer justification monitoring is disabled (default).
- 1 to *n* are the number of STSs on the port. One STS per port can be enabled from the PJSTSMon# card menu.

Figure 10-9 Enabling or Disabling Pointer Justification Count Parameters



Step 4 In the State field, confirm that the port is in service (IS).

Step 5 If the port is IS, click **Apply**. If the port is out of service (OOS, OOS_MT, OOS_AINS), select **IS** in the State field and click **Apply**.

Step 6 Click the **Performance** tab to view PM parameters. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Note The count fields for PPJC and NPJC PM parameters appear white and blank unless pointer justification count performance monitoring is enabled.

Step 7 Return to your originating procedure (NTP).

DLP-A122 Enable/Disable Intermediate Path Performance Monitoring

Purpose	This task enables or disables intermediate path performance monitoring, which allows you to monitor large amounts of STS traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. Far-end path monitoring can be performed on the OC3-4 and EC1 cards. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

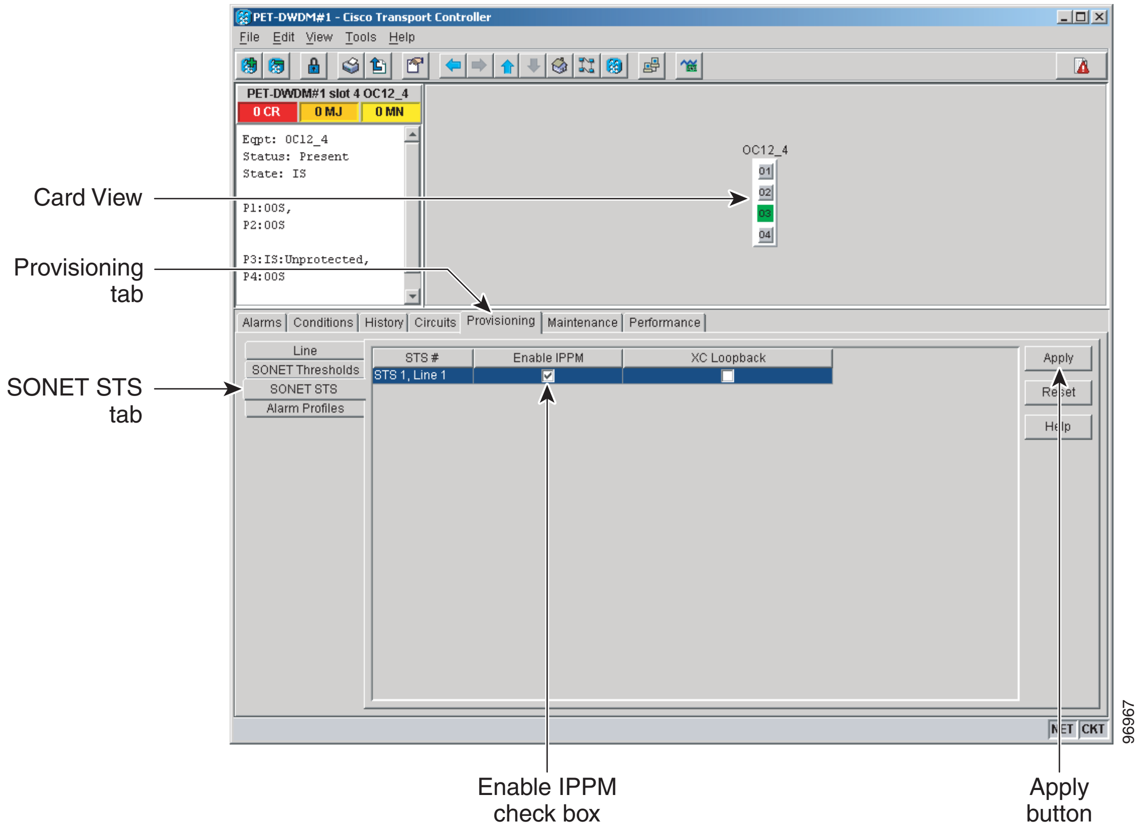
Note An OC-48 IR card used in a BLSR does not support IPPM during a protection switch.

Step 1 In node view, double-click the OC-*N* card you want to monitor. The card view appears.

See Table 10-2 on page 10-27 for a list of OC-*N* LTE cards.

Step 2 Click the **Provisioning > SONET STS** tabs (Figure 10-10).

Figure 10-10 SONET STS Tab for Enabling or Disabling IPPM



Step 3 Click the check box in the Enable IPPM column and make a selection based on the following rules:

- Unchecked means IPPM is disabled for that STS (default)
- Checked means IPPM is enabled for that STS

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

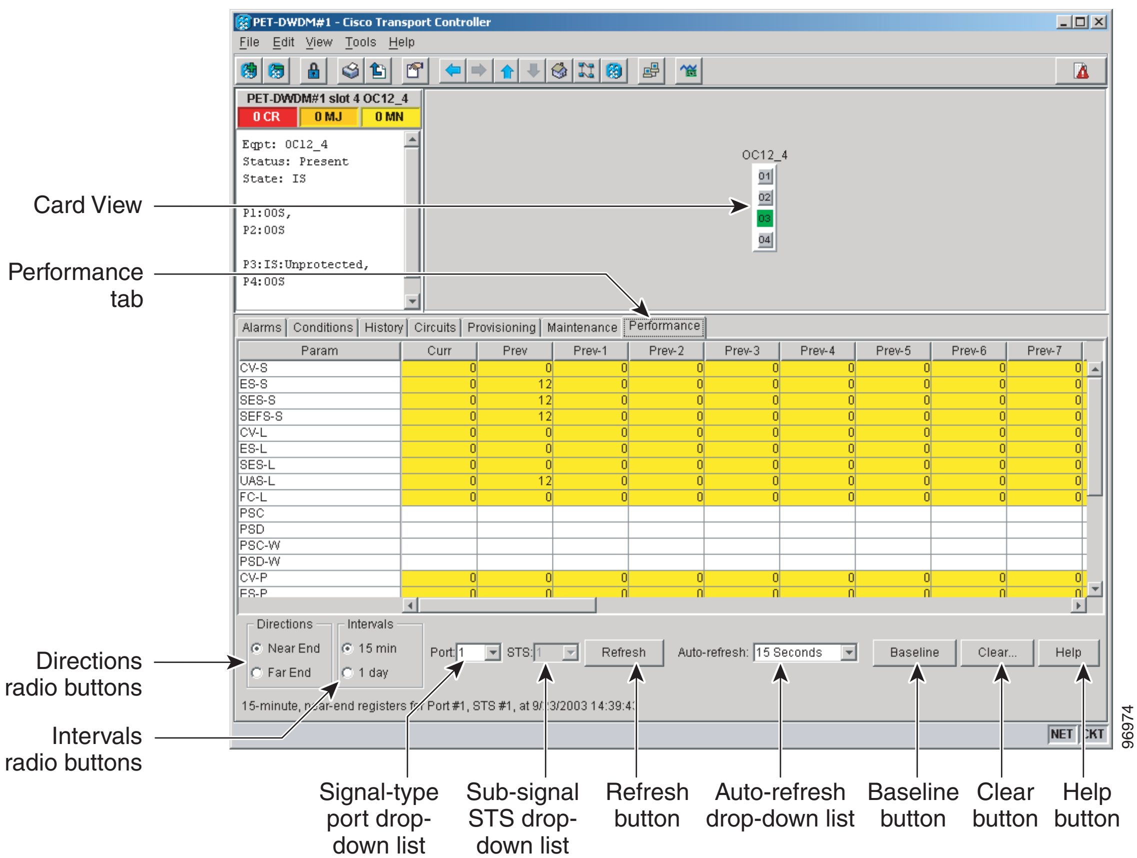
DLP-A507 View OC-N PM Parameters

Purpose	This task enables you to view PM counts on an OC-N card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the OC-N card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab (Figure 10-11).

Figure 10-11 Viewing OC-N Card Performance Monitoring Information



Step 3 In the Port drop-down menu, click the port you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down menu and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

NTP-A251 Monitor Multirate Transport Performance

Purpose	This procedure enables you to view node near-end or far-end performance during selected time intervals on a transponder (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G), or muxponder (MXP_2.5G_10G) card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A500 Enable/Disable OTN G.709 Performance Monitoring" task on page 10-33 as needed to enable or disable optical transport network (OTN) G.709 monitoring.

Step 3 Complete the "DLP-A501 Enable/Disable OTN FEC Performance Monitoring" task on page 10-34 as needed to enable or disable optical transport network (OTN) forward error correction (FEC) monitoring.

Step 4 Complete the "DLP-A317 View Optics PM Parameters" task on page 10-36 as needed.

Step 5 Complete the "DLP-A318 View Payload PM Parameters" task on page 10-37 as needed.

Step 6 Complete the "DLP-A319 View Optical Transport Network PM Parameters" task on page 10-39 as needed.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Stop. You have completed this procedure.

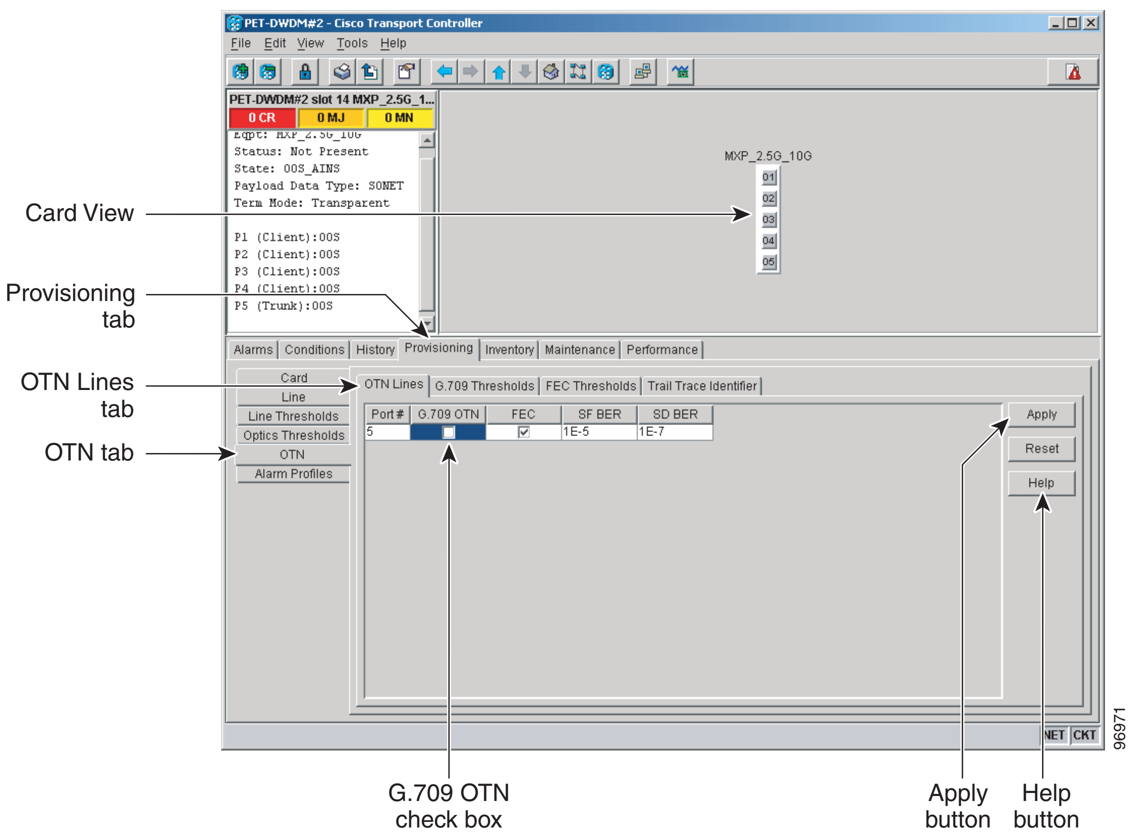
DLP-A500 Enable/Disable OTN G.709 Performance Monitoring

Purpose	This task enables or disables optical transport network (OTN) G.709 monitoring of near-end or far-end performance on a card and port during selected time intervals to detect possible problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card you want to monitor. The card view appears.

Step 2 Click the **Provisioning > OTN > OTN Lines** tabs (Figure 10-12).

Figure 10-12 OTN Lines Tab for Enabling/Disabling OTN G.709 Performance Monitoring



Step 3 Make a G.709 selection based on the following rules:

- Unchecked disables G.709 for that port (default)
- Checked enables G.709 for that port

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

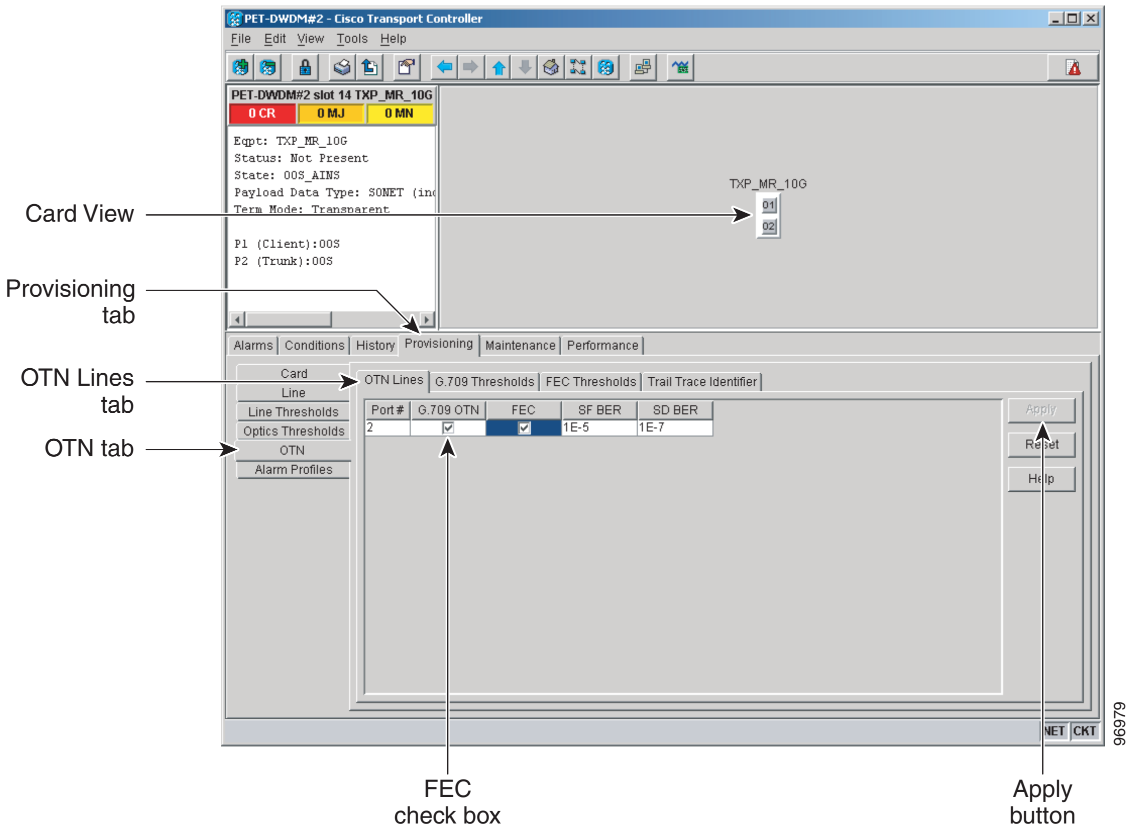
DLP-A501 Enable/Disable OTN FEC Performance Monitoring

Purpose	This task enables or disables optical transport network (OTN) FEC monitoring of node near-end or far-end performance on a selected card and port during selected time intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card you want to monitor. The card view appears.

Step 2 Click the **Provisioning > OTN > OTN Lines** tabs (Figure 10-13).

Figure 10-13 OTN Lines Tab for Enabling/Disabling OTN FEC Performance Monitoring



Step 3 Make an FEC selection based on the following rules:

- Unchecked disables FEC for that port (default)
- Checked enables FEC for that port

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

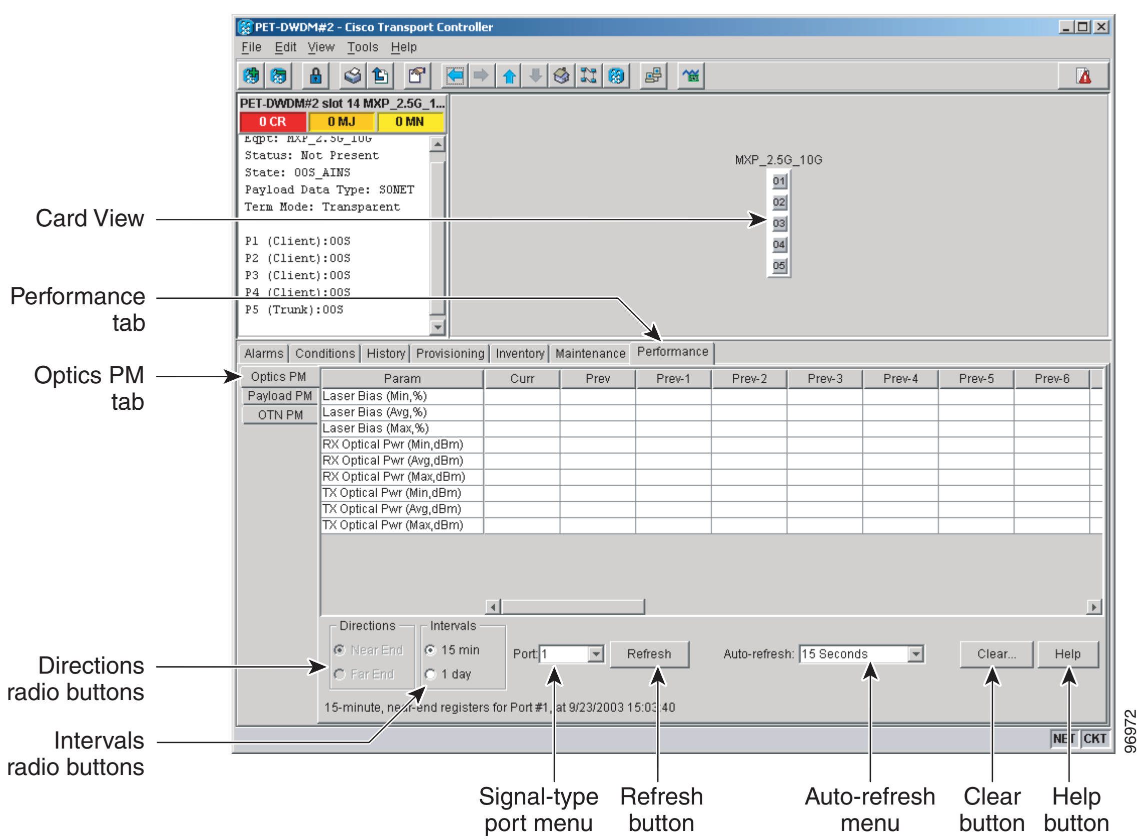
DLP-A317 View Optics PM Parameters

Purpose	This task enables you to view the optics PM counts on a transponder (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G), or muxponder (MXP_2.5G_10G) card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the transponder or muxponder card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Optics PM** tabs (Figure 10-14).

Figure 10-14 Viewing Optics Performance Monitoring Information



Step 3 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 4 Return to your originating procedure (NTP).

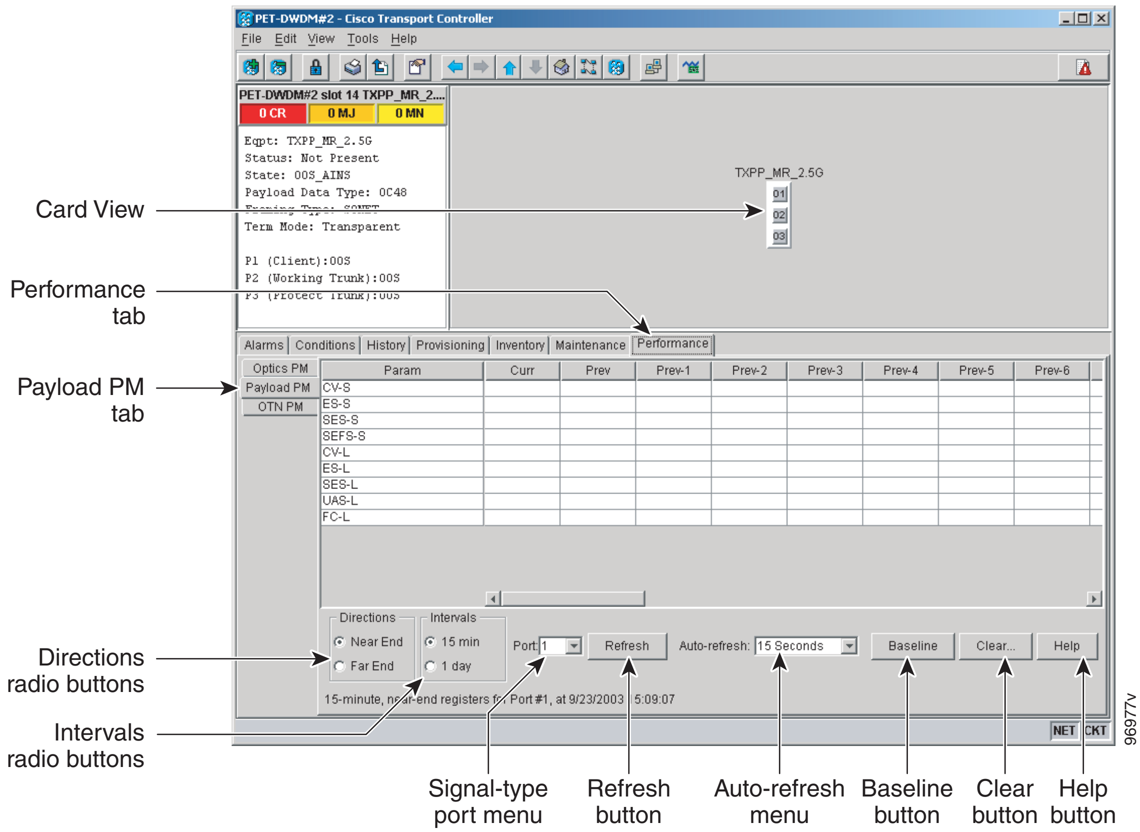
DLP-A318 View Payload PM Parameters

Purpose	This task enables you to view the payload PM counts on a transponder (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G), or muxponder (MXP_2.5G_10G) card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the transponder or muxponder card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Payload PM** tabs (Figure 10-15).

Figure 10-15 Viewing Payload Performance Monitoring Information



Step 3 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Note The PM parameters that appear depend on the data payload and framing type provisioned on the port. Unframed data payloads such as ESCON, DV6000, DSI/D1 video, and HDTV do not provide payload performance monitoring information.

Step 4 Return to your originating procedure (NTP).

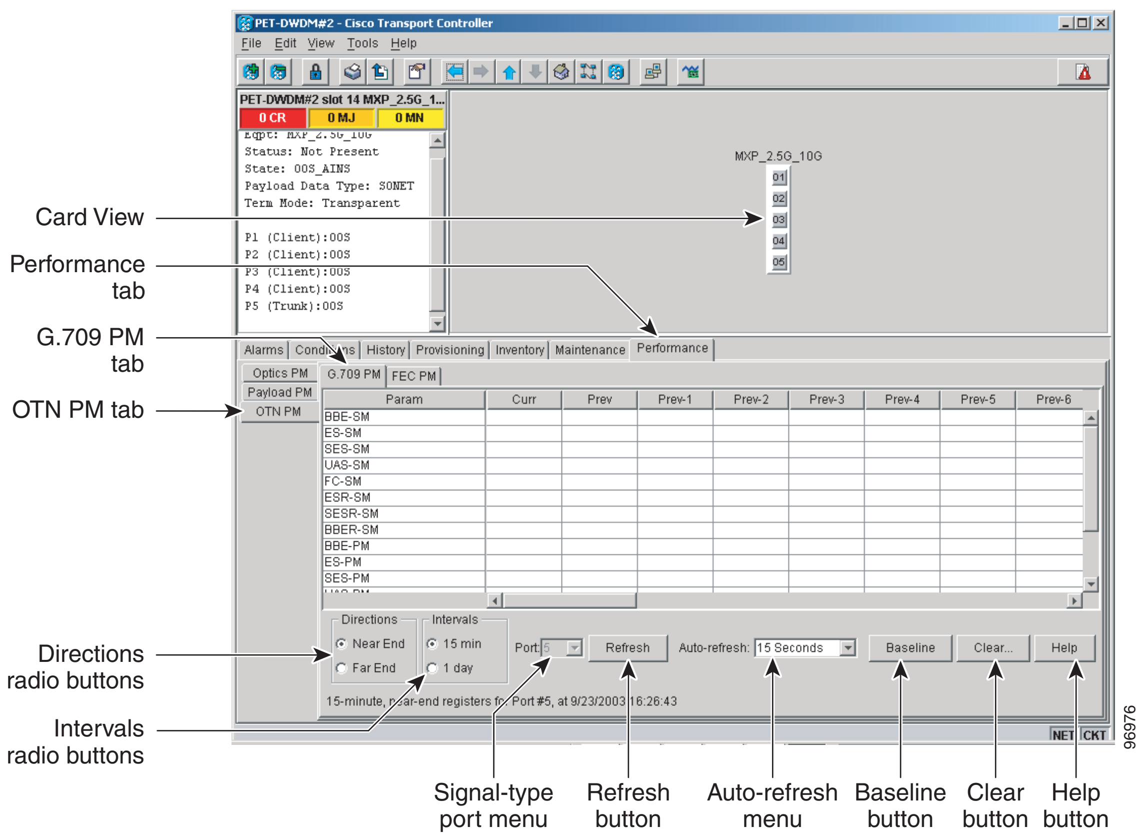
DLP-A319 View Optical Transport Network PM Parameters

Purpose	This task enables you to view the optical transport network (OTN) PM counts on a transponder (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G), or muxponder (MXP_2.5G_10G) card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the transponder or muxponder card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > OTN PM > G.709** tabs (Figure 10-16).

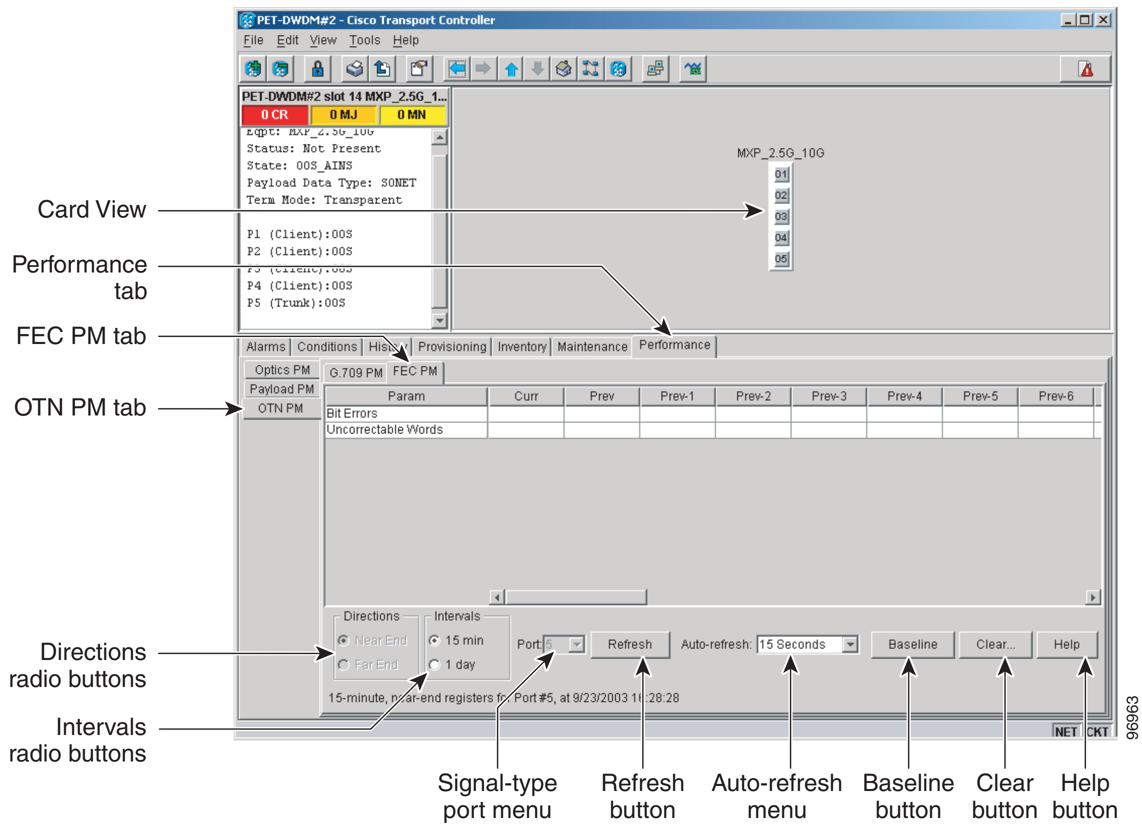
Figure 10-16 Viewing OTN G.709 Performance Monitoring Information



Step 3 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 4 Click the **FEC PM** tab (Figure 10-17).

Figure 10-17 Viewing OTN FEC Performance Monitoring Information



Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

NTP-A252 Monitor DWDM Performance

Purpose	This procedure enables you to view transmit and receive performance during selected time intervals on a DWDM card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A502 View Optical Service Channel PM Parameters" task on page 10-41.

Step 3 Complete the "DLP-A503 View Optical Amplifier PM Parameters" task on page 10-42.

Step 4 Complete the "DLP-A504 View Optical Multiplexer and Demultiplexer PM Parameters" task on page 10-44.

Step 5 Complete the "DLP-A505 View Channel Filter Optical Add/Drop Multiplexer PM Parameters" task on page 10-45.

Step 6 Complete the "DLP-A506 View Band Filter Optical Add/Drop Multiplexer PM Parameters" task on page 10-46.

To refresh, reset, or clear PM counts, see the "NTP-A253 Change the PM Display" procedure on page 10-2.

Stop. You have completed this procedure.

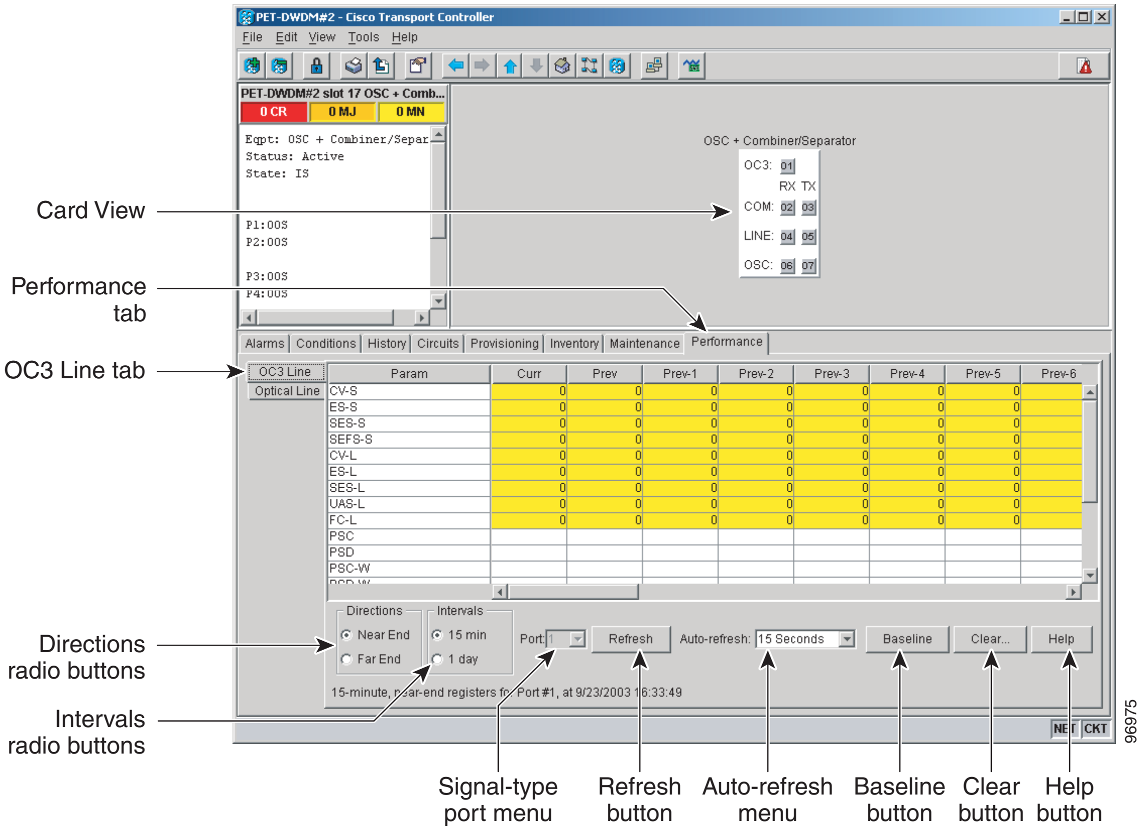
DLP-A502 View Optical Service Channel PM Parameters

Purpose	This task enables you to view optical service channel PM counts at selected time intervals on an OSCM or OSC-CSM card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the OSCM or OSC-CSM card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > OC3 Line** tabs (Figure 10-18).

Figure 10-18 OC3 Line Tab in the Optical Service Channel Card View Performance Window



Step 3 Click **Refresh**. OC3 line performance monitoring statistics for the selected port appear.

Step 4 Click the **Optical Line** tab.

Step 5 Click **Refresh**. Optical line performance monitoring statistics for the selected port appear.

Step 6 Return to your originating procedure (NTP).

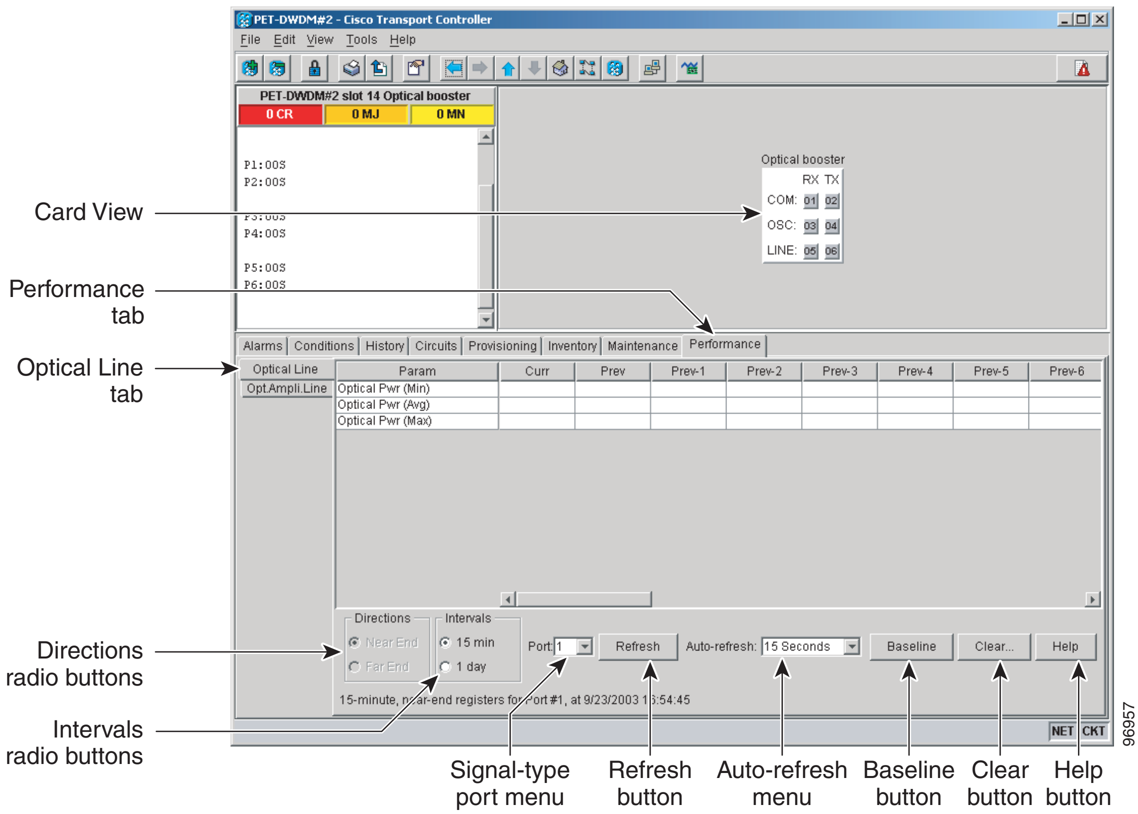
DLP-A503 View Optical Amplifier PM Parameters

Purpose	This task enables you to view optical amplifier PM counts at selected time intervals on an OPT PRE or OPT BST card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the optical amplifier card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Optical Line** tabs (Figure 10-19).

Figure 10-19 Optical Line Tab in the Optical Amplifier Card View Performance Window



Step 3 Click **Refresh**. Optical line performance monitoring statistics for the selected port appear.

Step 4 Click the **Opt. Ampli. Line** tab.

Step 5 Click **Refresh**. Optical amplifier line performance monitoring statistics for the selected port appear.

Step 6 Return to your originating procedure (NTP).

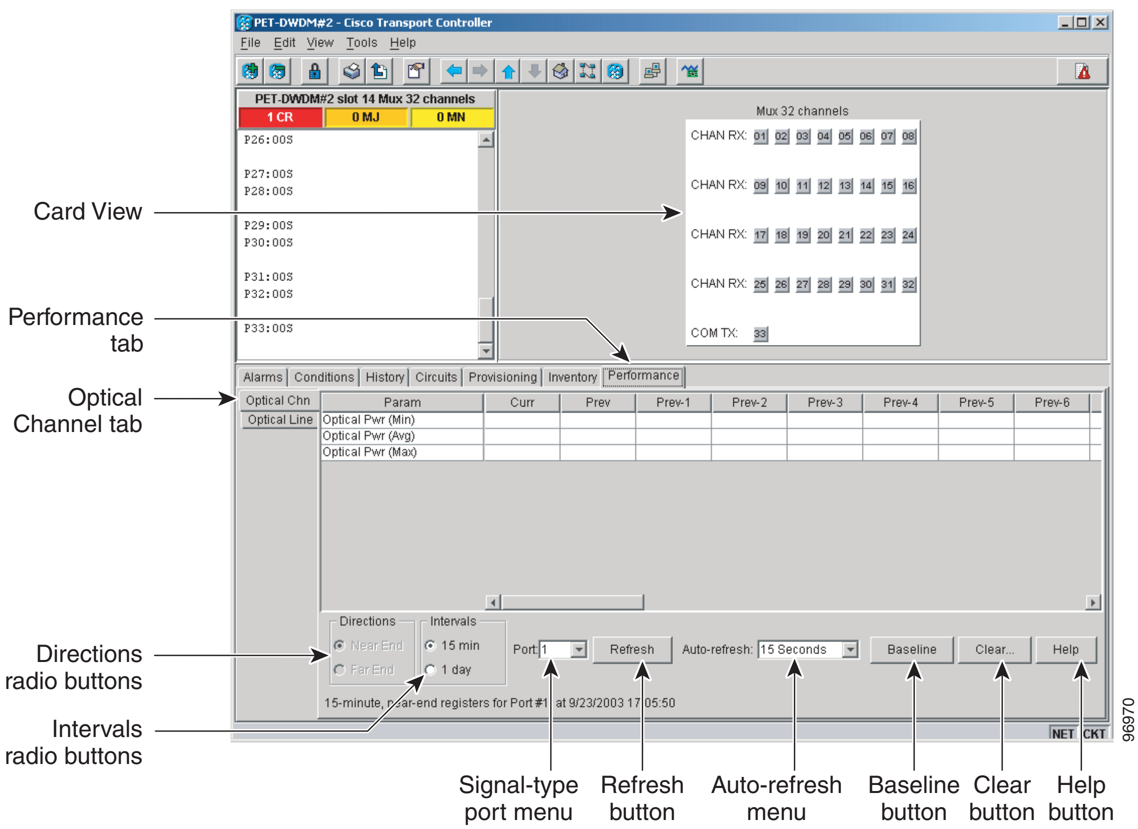
DLP-A504 View Optical Multiplexer and Demultiplexer PM Parameters

Purpose	This task enables you to view multiplexer or demultiplexer PM counts at selected time intervals on a 32MUX or 32DMX card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 32MUX or 32DMX card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Optical Chn** tabs (Figure 10-20).

Figure 10-20 Optical Channel Tab in the Mux/Demux Card View Performance Window



Step 3 Click **Refresh**. Optical channel performance monitoring statistics for the selected port appear.

Step 4 Click the **Optical Line** tab.

Step 5 Click **Refresh**. Optical line performance monitoring statistics for the selected port appear.

Step 6 Return to your originating procedure (NTP).

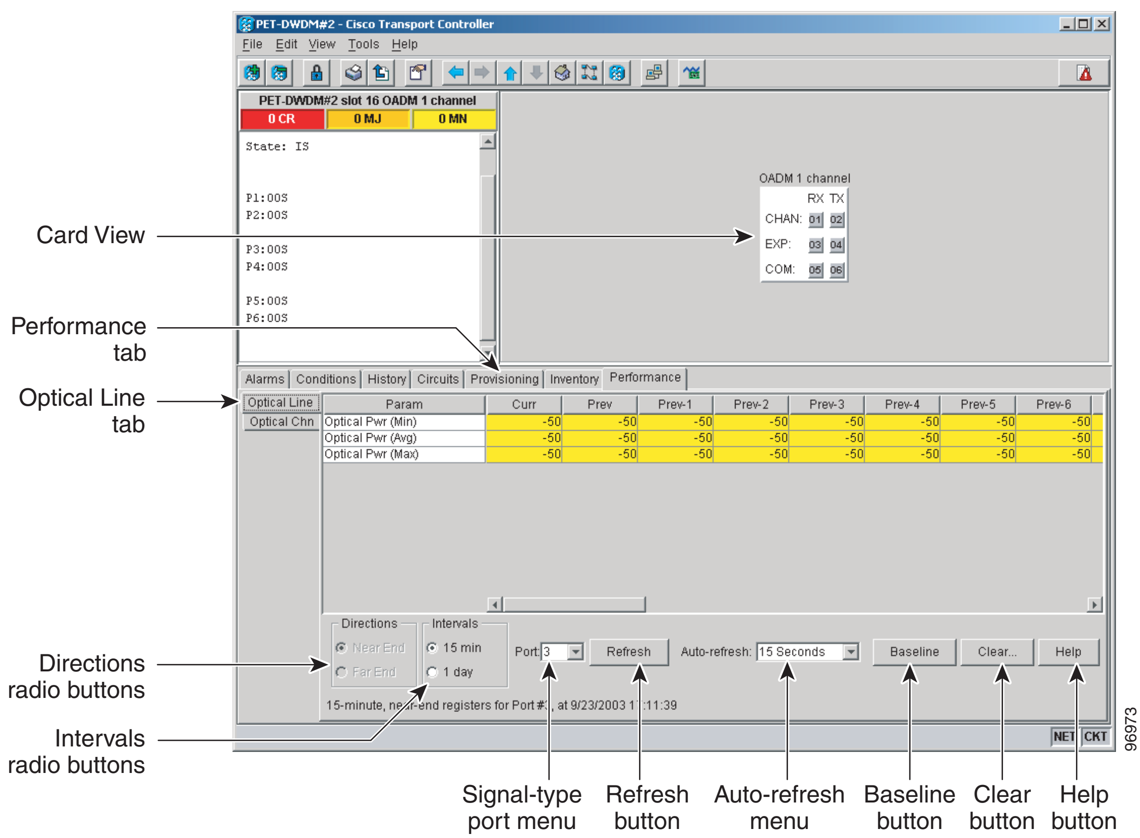
DLP-A505 View Channel Filter Optical Add/Drop Multiplexer PM Parameters

Purpose	This task enables you to view optical add/drop channel multiplexer PM counts at selected time intervals on an AD1C, AD2C, or AD4C card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the optical add/drop channel multiplexer card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Optical Line** tabs (Figure 10-21).

Figure 10-21 Optical Line Tab in the Channel Filter OADM Card View Performance Window



Step 3 Click **Refresh**. Optical line performance monitoring statistics for the selected port appear.

Step 4 Click the **Optical Chn** tab.

Step 5 Click **Refresh**. Optical channel performance monitoring statistics for the selected port appear.

Step 6 Return to your originating procedure (NTP).

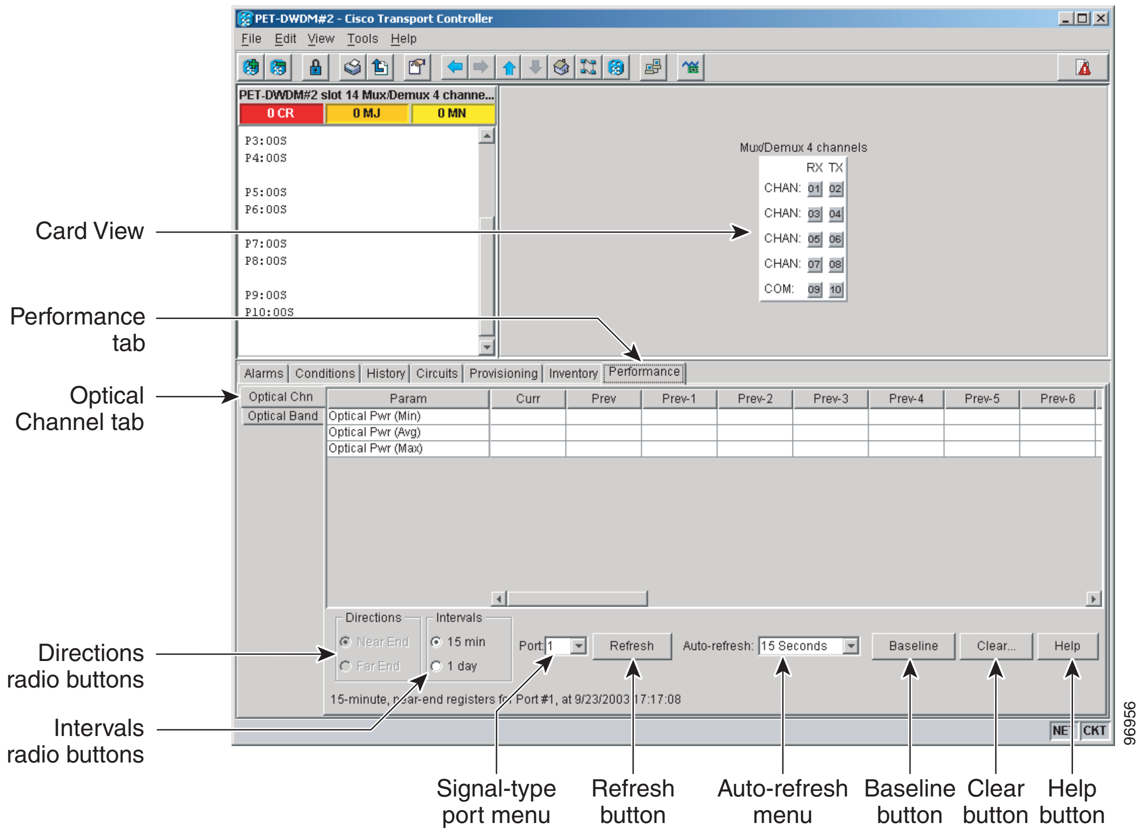
DLP-A506 View Band Filter Optical Add/Drop Multiplexer PM Parameters

Purpose	This task enables you to view optical add/drop band multiplexer PM counts at selected time intervals on an AD1B, AD4B, or 4MD card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the optical add/drop band multiplexer card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **Optical Chn** tabs (Figure 10-22).

Figure 10-22 Optical Channel Tab in the Card View Performance Window



Step 3 Click **Refresh**. Optical channel performance monitoring statistics for the selected port appear.

Step 4 Click the **Optical Band** tab.

Step 5 Click **Refresh**. Optical band performance monitoring statistics for the selected port appear.

Step 6 Return to your originating procedure (NTP).

NTP-A285 Monitor FC_MR-4 Performance

Purpose	This procedure enables you to view node transmit and receive performance during selected time intervals on a FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 8, "Create Circuits and VT Tunnels" and Chapter 13, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A350 View FC_MR-4 Statistics PM Parameters" task on page 10-48.

Step 3 Complete the "DLP-A351 View FC_MR-4 Utilization PM Parameters" task on page 10-49.

Step 4 Complete the "DLP-A352 View FC_MR-4 History PM Parameters" task on page 10-50.

Stop. You have completed this procedure.

DLP-A350 View FC_MR-4 Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Statistics** tabs.

Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

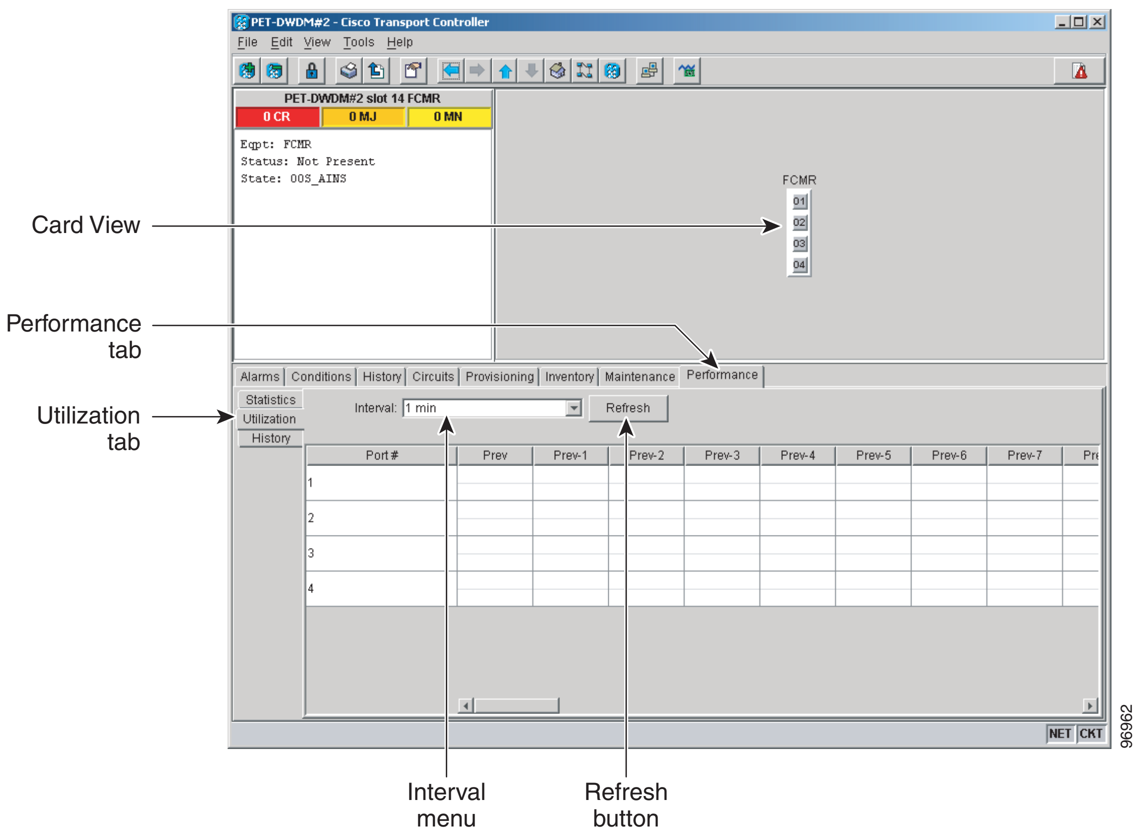
DLP-A351 View FC_MR-4 Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance > Utilization** tabs (Figure 10-23).

Figure 10-23 FC_MR-4 Utilization on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column to find the port you want to monitor.

Step 5 The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

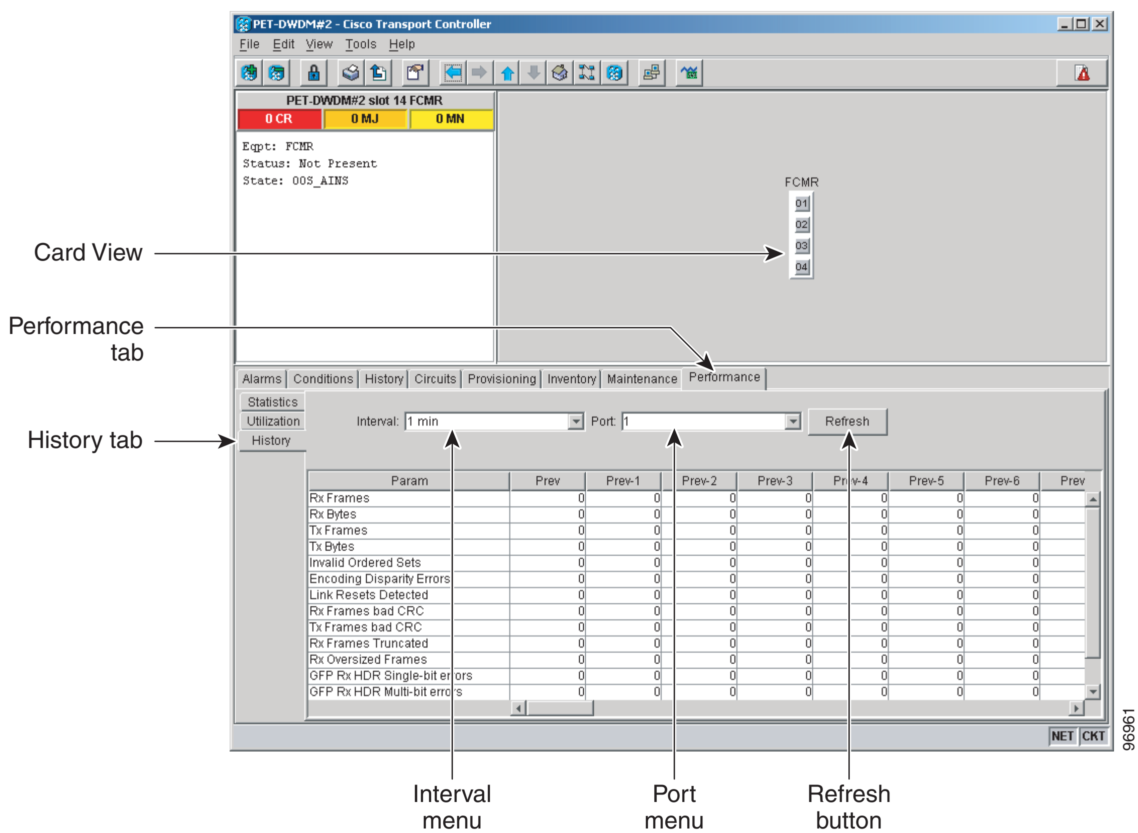
DLP-A352 View FC_MR-4 History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an FC_MR-4 card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** > **History** tabs (Figure 10-24).

Figure 10-24 FC_MR-4 History on the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring statistics for each port on the card appear.

Step 4 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A353 Refresh FC_MR-4 PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Utilization** or the **History** tab.

Step 4 From the Interval drop-down menu, choose one of four options:

- 1 min: This option appears the specified PM counts in one-minute time intervals.
- 15 min: This option appears the specified PM counts in 15-minute time intervals.
- 1 hour: This option appears the specified PM counts in one-hour time intervals.
- 1 day: This option appears the specified PM counts in one-day (24 hours) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the selected time interval.

Step 6 Return to your originating procedure (NTP).

NTP-A289 Create or Delete FC_MR-4 RMON Thresholds

Purpose	Use this procedure to create or delete FC_MR-4 remote monitoring (RMON) thresholds for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Perform any of the following tasks as needed:

- DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 10-52
- DLP-A358 Delete FC_MR-4 RMON Alarm Thresholds, page 10-54

Stop. You have completed this procedure.

DLP-A357 Create FC_MR-4 RMON Alarm Thresholds

Purpose	This procedure sets up remote monitoring (RMON) to allow network management systems to monitor FC_MR-4 ports. This procedure does not apply to DWDM nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to set up RMON. If you are already logged in, continue with Step 2.

Step 2 Double-click the FC_MR-4 card where you want to create the RMON alarm thresholds.

Step 3 In card view, click the **Provisioning** > **Line Thresholds** tabs.

Step 4 Click **Create**. The Create FCMR Threshold dialog box appears.

Step 5 From the Slot menu, choose the appropriate FC_MR-4 card.

Step 6 From the Port drop-down menu, choose the applicable port on the FC_MR-4 card you selected.

Step 7 From the Variable drop-down menu, choose the variable. See Table 10-3 for a list of the FC_MR-4 threshold variables available in this field.

Table 10-3 FC_MR-4 Threshold Variables (MIBs)

Variable	Definition
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined fibre channel control words.
fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.
fibreStatsRxFramesTooLong	Received oversize fibre channel frames > 2148 including CRC.
fibreStatsRxFramesBadCRC	Received fibre channel frames with bad CRC.
fibreStatsRxFrames	Received total fibre channel frames.
fibreStatsRxOctets	Received total fibre channel data bytes within a frame.
fibreStatsTxFramesBadCRC	Transmitted fibre channel frames with bad CRC.

Table 10-3 FC_MR-4 Threshold Variables (MIBs) (continued)

Variable	Definition
fibreStatsTxFrames	Transmitted total fibre channel frames.
fibreStatsTxOctets	Transmitted total fibre channel data bytes within a frame.
fibreStatsLinkResets	Total number of link resets initiated by FCMR port when link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received GFP (generic framing protocol) frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect fibre channel data.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain fibre channel data.

Step 8 From the Alarm Type drop-down menu, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 9 From the Sample Type drop-down menu, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

Step 10 Type in an appropriate number of seconds for the Sample Period.

Step 11 Type in the appropriate number of occurrences for the Rising Threshold.

Note For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, the excess occurrences trigger an alarm.

Step 12 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15 minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 13 Click **OK** to complete the procedure.

Step 14 Return to your originating procedure (NTP).

DLP-A358 Delete FC_MR-4 RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 10-52
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the FC_MR-4 card where you want to delete the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning** > **Line Thresholds** tabs.

Step 3 Click the RMON alarm threshold you want to delete.

Step 4 Click **Delete**. The Delete Threshold dialog box opens.

Step 5 Click **Yes** to delete that threshold.

Step 6 Return to your originating procedure (NTP).

CHAPTER 11

Manage Circuits

This chapter explains how to manage Cisco ONS 15454 electrical, optical (OC-N), Ethernet, and virtual concatenated (VCAT) circuits. It also explains how to manage optical channel network connections provisioned in dense wavelength division multiplexing (DWDM) networks.

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.

Before You Begin

To create circuits, see Chapter 8, "Create Circuits and VT Tunnels."

To clear any alarm or trouble conditions, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A199 Locate and View Circuits, page 11-2—Complete as needed.
2. NTP-A200 View Cross-Connect Card Resource Usage, page 11-11—Complete as needed.
3. NTP-A151 Modify and Delete Circuits, page 11-12—Complete as needed to edit a circuit name; change the active and standby colors of spans; change signal fail, signal degrade thresholds, reversion time, and PDI-P settings for path protection circuits; or delete a circuit or DWDM optical channel connection.
4. NTP-A278 Modify and Delete Overhead Circuits, page 11-19—Complete as needed to change a tunnel type, repair an IP circuit, or delete overhead circuits.
5. NTP-A416 Convert a CTC Circuit to TL1 Cross-Connects, page 11-22—Complete this procedure if you want to convert a CTC circuit into TL1 cross-connects.
6. NTP-A417 Upgrade TL1 Cross-Connects to CTC Circuits, page 11-23—Complete this procedure if you want to convert TL1 cross-connects or TL1-like cross-connects created in CTC into a CTC circuit.
7. NTP-A78 Create a Monitor Circuit, page 11-24—Complete as needed to monitor traffic on primary bidirectional circuits.
8. NTP-A79 Create a J1 Path Trace, page 11-25—Complete as needed to monitor interruptions or changes to circuit traffic.

NTP-A199 Locate and View Circuits

Purpose	This procedure allows you to locate and view circuits, DWDM optical channel network connections, and spanning tree information.
Tools/Equipment	None
Prerequisite Procedures	Circuit creation procedure(s) in Chapter 8, "Create Circuits and VT Tunnels"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you want to view the circuits. If you are already logged in, continue with Step 2.

Note Do not check Disable Circuit Management on the Login dialog box. No circuits appear if this option is checked.

Step 2 As needed, complete the "DLP-A416 View Circuit Information" task on page 11-2.

Step 3 As needed, complete the "DLP-A131 Search for Circuits" task on page 11-6.

Step 4 As needed, complete the "DLP-A262 Filter the Display of Circuits" task on page 11-7.

Step 5 As needed, complete the "DLP-A229 View Circuits on a Span" task on page 11-9.

Step 6 As needed, complete the "DLP-A417 View the BLSR Squelch Table" task on page 11-10.

Step 7 As needed, complete the "DLP-A430 View Spanning Tree Information" task on page 11-11.

Stop. You have completed this procedure.

DLP-A416 View Circuit Information

Purpose	This task provides information about ONS 15454 circuits and DWDM optical channel network connections.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To view circuits for an entire network, from the View menu, choose **Go to Network View**.
- To view circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.

- To view circuits that originate, terminate, or pass through a specific card, in node view, double-click the card containing the circuits you want to view.

Note In node or card view, you can change the scope of the circuits that appear by choosing Card (in card view), Node, or Network from the Scope drop-down menu in the bottom right corner of the Circuits window.

Step 2 Click the **Circuits** tab. The Circuits tab shows the following information:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—Circuit types are: STS (STS circuit), VT (VT circuit), VTT (VT tunnel), VAP (VT aggregation point), OCHNC (DWDM optical channel network connection), STS-v (STS VCAT circuit), or VT-v (VT VCAT circuit).
- Size—Circuit size. VT circuits are 1.5. STS circuit sizes are 1, 3c, 6c, 9c, 12c, 24c, 48c, 192c. OCHNC sizes are Equipped not specific, Multi-rate, 2.5 Gbps No FEC (forward error correction), 2.5 Gbps FEC, 10 Gbps No FEC, and 10 Gbps FEC. VCAT circuits are STS-1-2v, STS-3c-2v, or STS-12c-2v.
- OCHNC Wlen—For OCHNCs, the wavelength provisioned for the optical channel network connection. See Table 5-6 on page 5-20 for a list of channels and wavelengths.
- Direction—The circuit direction, either two-way or one-way.
- OCHNC Dir—For OCHNCs, the direction of the optical channel network connection, either east to west or west to west.
- Protection—The type of circuit protection. See Table 11-1 for a list of protection types.

Table 11-1 Circuit Protection Types

Protection Type	Description
N/A	Circuit protection is not applicable.
2F BLSR	The circuit is protected by a two-fiber bidirectional line switched ring (BLSR).
4F BLSR	The circuit is protected by a four-fiber BLSR.
BLSR	The circuit is protected by a both a two-fiber and a four-fiber BLSR.
Path Protection	The circuit is protected by a path protection.
Path Protection-DRI	The circuit is protected by a path protection dual ring interconnection.
1+1	The circuit is protected by a 1+1 protection group.
Y-Cable	The circuit is protected by a transponder or muxponder card Y-cable protection group.
Splitter	The circuit is protected by the protect transponder (TXPP_MR_2.5G) splitter protection.
Protected	The circuit is protected by diverse SONET topologies, for example, a BLSR and a path protection, or a path protection and 1+1.
2F-PCA	The circuit is routed on a protection channel access (PCA) path on a two-fiber BLSR. PCA circuits are unprotected.
4F-PCA	The circuit is routed on a protection channel access path on a four-fiber BLSR. PCA circuits are unprotected.

Table 11-1 Circuit Protection Types (continued)

Protection Type	Description
PCA	The circuit is routed on a protection channel access path on both two-fiber and four-fiber BLSRs. PCA circuits are unprotected.
Unprot (black)	The circuit is not protected.
Unprot (red)	A circuit created as a fully-protected circuit is no longer protected due to a system change, such as removal of a BLSR or 1+1 protection group.
Unknown	Circuit protection types appear in the Protection column only when all circuit components are known, that is, when the circuit status is ACTIVE or UPGRADABLE. If the circuit is in some other status, the protection type is "unknown."

- Status—The circuit status. Table 11-2 lists the circuit statuses that can appear.

Table 11-2 Cisco ONS 15454 Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
ACTIVE	CTC created a circuit. All components are in place and a complete path exists from the circuit source to the circuit destination.
DELETING	CTC is deleting a circuit.
INCOMPLETE	A CTC-created circuit is missing a cross-connect or network span, a complete path from source to destination(s) does not exist, or an Alarm Interface Panel (AIP) change occurred on one of the circuit nodes and the circuit is in need of repair. (AIPs store the node MAC address.) In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is INCOMPLETE. However, an INCOMPLETE status does not necessarily mean a circuit traffic failure has occurred, because traffic may flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans are shown as green lines, and down spans are shown as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line will not appear on the network map. Subsequently, circuits routed on a network span that goes down will appear as ACTIVE during the current CTC session, but they will appear as INCOMPLETE to users who log in after the span failure. The INCOMPLETE status does not appear for OCHNC circuit types.

Table 11-2 Cisco ONS 15454 Circuit Status (continued)

Status	Definition/Activity
UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete and has upgradable cross-connects. A complete path from source to destination(s) exists. You can upgrade the circuit using the "NTP-A417 Upgrade TL1 Cross-Connects to CTC Circuits" procedure on page 11-23. This status does not appear for OCHNC circuit types.
INCOMPLETE_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit with upgradable cross-connects is missing a cross-connect, and a complete path from source to destination(s) does not exist. The circuit cannot be upgraded until missing cross-connects are in place. This status does not appear for OCHNC circuit types.
NOT_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete but has at least one non-upgradable cross-connect. UPSR_HEAD, UPSR_EN, UPSR_DC, and UPSR_DROP cross-connects are not upgradable, so all unidirectional path protection circuits created with TL1 are not upgradable. This status does not appear for OCHNC circuit types.
INCOMPLETE_NOT_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit with one or more non-upgradable cross-connects is missing a connection or circuit span (network link); a complete path from source to destination(s) does not exist. This status does not appear for OCHNC circuit types.

- Source—The circuit source in the format: node/slot/port "port name"/STS/VT. (The port name will appear in quotes.) Node and slot will always appear; port "port name"/STS/VT might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the circuit size is a concatenated size (3c, 6c, 12c, etc.), STSs used in the circuit will be indicated by an ellipsis, for example, "S7..9," (STSs 7, 8, and 9) or S10..12 (STS 10, 11, and 12).
- Destination—The circuit destination in same format (node/slot/port "port name"/STS/VT) as the circuit source.
- # of VLANS—The number of VLANS used by an Ethernet circuit.
- # of Spans—The number of inter-node links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose to show or hide circuit span detail.
- State—The circuit state Table 11-3 lists the circuit states that may appear.

Table 11-3 Cisco ONS 15454 Circuit States

State	Definition
IS	In service; able to carry traffic.
OOS	Out of service; unable to carry traffic. This status does not appear for OCHNC circuit types.

Table 11-3 Cisco ONS 15454 Circuit States (continued)

State	Definition
OOS-AINS	Out of service, auto in service; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. VT circuits in OOS-AINS generally switch to IS when source and destination ports are IS, OOS-AINS, or OOS-MT regardless of whether a physical signal is present. STS circuits in OOS-AINS switch to IS when a signal is received. This status does not appear for OCHNC circuit types.
OOS-MT	Out of service, maintenance; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. This status does not appear for OCHNC circuit types.

Step 3 Return to your originating procedure (NTP).

DLP-A131 Search for Circuits

Purpose	This task searches for ONS 15454 circuits and DWDM optical channel network connections at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To search the entire network, from the View menu, choose **Go to Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 If you are in node or card view, choose the scope for the search (**Network** or **Node**) in the Scope drop-down menu.

Step 4 Click **Search**.

Step 5 In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match whole word only—Check this check box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.

- Match case—Check this check box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 6 Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.

Step 7 Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-A262 Filter the Display of Circuits

Purpose	This task filters the display of circuits and DWDM optical channel network connections in the Circuits window. You can filter the circuits in network, node, or card view based on circuit or OCHNC name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To filter network circuits, from the View menu, choose **Go to Network View**.
- To filter circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 Set the attributes for filtering the circuit display:

a. Click the **Filter** button.

b. In the Circuit Filter dialog box, set the filter attributes by choosing one or more of the following:

  - Name—Enter a complete or partial circuit name to filter circuits based on the circuit name; otherwise leave the field blank.
  - Direction—Choose one: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).
  - OCHNC Dir—(DWDM optical channel network connections only) Choose one: **East to West** (displays only east-to-west circuits); **West to East** (displays only west-to-east circuits).
  - OCHNC Wlen—(DWDM optical channel network connections only) Choose an OCHNC wavelength to filter the circuits. For example, choosing 1530.33 will display channels provisioned on the 1530.33 nm wavelength.

- Status—Choose one: **Any** (status not used to filter circuits), **Active** (display only active circuits; optical channel network connections have Active status only), **Incomplete** (display only incomplete circuits, that is, circuits missing a connection or span to form a complete path), or **Upgradable** (display only upgradable circuits, that is, circuits created in TL1 that are ready to upgrade in CTC). See Table 11-2 for more information about circuit statuses. Although other statuses are described in the table, filtering is only supported for Active, Incomplete, and Upgradable circuits.
- State—Choose one: **OOS** (display only out-of-service circuits), **IS** (display only in-service circuits; optical channel network connections have IS status only), **OOS-AINS** (display only out-of-service, auto in-service circuits), or **OOS-MT** (display only out-of-service, maintenance circuits.) See Table 11-3 for more information about circuit states.
- Slot—Enter a slot number to filter circuits based on the source or destination slot; otherwise leave the field blank.
- Port—Enter a port number to filter circuits based on the source or destination port; otherwise leave the field blank.
- Type—Choose one: **Any** (type not used to filter circuits), **STS** (displays only STS circuits), **VT** (displays only VT circuits), **VT Tunnel** (displays only VT tunnels), **STS-V** (displays STS VCAT circuits), **VT-V** (displays VT VCAT circuits), **VT Aggregation Point** (displays only VT aggregation points), or **OCHNC** (displays only optical channel network connections).
- Size—Click the appropriate check boxes to filter circuits based on size: VT1.5, STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, STS-192c, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, or 10 Gbps No FEC.

  The check boxes shown depend on the Type field selection. If you chose Any, all sizes are available. If you chose VT, only VT1.5 is available. If you chose STS, only STS sizes are available, and if you chose VT Tunnel or VT Aggregation Point, only STS-1 is available. If you chose OCHNC as the circuit type, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, and 10 Gbps No FEC appear. If you chose STS-V, only STS-1, STS3c, and STS-12c are available. If you chose VT-V, only VT1.5 is available.

Step 4 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.

Step 5 To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the **Filter** button to change the filter attributes.

Step 6 Return to your originating procedure (NTP).

DLP-A229 View Circuits on a Span

Purpose	This task allows you to view circuits and DWDM optical channel network connections on an ONS 15454 span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span. See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures. DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu on the node view, choose **Go to Network View**. If you are already in network view, continue with Step 2.

Step 2 Right-click the green line containing the circuits you want to view and choose one of the following:

- Circuits—To view BLSR, path protection, 1+1, VCAT, DWDM optical channel network connections, or unprotected circuits on the span.
- PCA Circuits—To view circuits routed on a BLSR protected channel. (This option does not appear if the span you right-clicked is not a BLSR span.)

In the Circuits on Span dialog box, you can view the following information about the circuits that traverse the span. The information that appears depends on the circuit type.

For OC-N, VCAT, DS-1, and DS-3 circuits provisioned on the span, the following information appears:

- STS—Displays STSs used by the circuits.
- VT—Displays VTs used by the circuits (VT circuits).
- UPSR—(path protection span only) If checked, path protection circuits are on the span.
- Circuit—Displays the circuit name.
- Switch State—(path protection span only) Displays the switch state of the circuit, that is, whether any span switches are active. For path protection spans, switch types include: CLEAR (no spans are switched), MANUAL (a manual switch is active), FORCE (a force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

Note You can perform other procedures from the Circuits on Span dialog box. If the span is in a path protection, you can switch the span traffic. See "DLP-A197 Initiate a Path Protection Force Switch" task on page 16-16 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-A231 Edit a Circuit Name" task on page 11-14 or the "DLP-A233 Edit Path ProtectionCircuit Path Selectors" task on page 11-16 for instructions.

For DWDM optical channel network connections, the following information appears:

- OCHNC Wavelength—The wavelength provisioned for the optical channel network connection.
- OCHNC Dir—The direction provisioned for the optical channel network connection, either east to west or west to east.
- Circuit—The optical channel network connection circuit name.

Step 3 Return to your originating procedure (NTP).

DLP-A417 View the BLSR Squelch Table

Purpose	This task allows you to view the BLSR squelch table for an ONS 15454 BLSR node. The table shows STSs that will be squelched for every isolated node. Squelching replaces traffic by the appropriate path alarm indication signal (AIS); it prevents traffic misconnections when a working channel service contends for access to a protection channel time slot carrying extra traffic. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Provisioning > BLSR tabs**.

Step 2 Click the BLSR whose squelch table you want to view.

Step 3 Click **Squelch Table**. In the BLSR Squelch Table window you can view the following information:

- STS Number—Shows the BLSR STS numbers. For two-fiber BLSRs, the number of STSs is half the BLSR OC-N, for example, an OC-48 BLSR squelch table will show 24 STSs. For four-fiber BLSRs, the number of STSs in the table is the same as the BLSR OC-N.
- West Source—If traffic is received by the node on its west span, the BLSR node ID of the source appears. (To view the BLSR node IDs for all nodes in the ring, click the **Ring Map** button.)
- West Dest—If traffic is sent on the node's west span, the BLSR node ID of the destination appears.
- East Source—If traffic is received by the node on its east span, the BLSR node ID of the source appears.
- East Dest—If traffic is sent on the node's east span, the BLSR node ID of the destination appears.

Note BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to or from E-Series Ethernet cards provisioned in a multicard Ethergroup.

Step 4 Return to your originating procedure (NTP).

DLP-A430 View Spanning Tree Information

Purpose	This task allows you to view E-Series Ethernet circuits and the Ethernet front ports operating with the spanning tree protocol (STP). The E-Series card supports up to eight STPs per node. For more information about the spanning tree protocol, refer to the *Cisco ONS 15454 Reference Manual*.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > EtherBridge > Circuits** tabs.

Step 2 In the EtherBridge Circuits window you can view the following information:

- Type—Identifies the type of Ethernet circuit mapped to the spanning tree, such as EtherSwitch point-to-point.
- Circuit Name/Port—Identifies the circuit name for the circuit in the spanning tree. This column also lists the Ethernet slots and ports mapped to the spanning tree for the node.
- STP ID—Shows the spanning tree protocol ID number.
- VLANS—Lists the VLANs associated with the circuit or port.

Step 3 Return to your originating procedure (NTP).

NTP-A200 View Cross-Connect Card Resource Usage

Purpose	This procedure allows you to view the percentage of cross-connect card resources used by circuits that traverse or terminate at an ONS 15454. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	XC, XCVT, or XC10G cards must be installed.
Prerequisite Procedures	DLP-A37 Install the XC, XCVT, or XC10G Cards, page 2-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to view the cross-connect card resource usage. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Cross-Connect > Resource Usage** tabs.

Step 3 In the Summary area of the Resources Usage tab, view the following information:

- STS-1 Matrix—(XC, XCVT, XC10G) Provides the percent of the cross-connect card STS-1 path resources that are in use. 288 STS-1 paths are available for XC or XCVT cards; 1152 STS-1 paths are available for XC10G cards.

- VT Matrix Ports—(XCVT and XC10G) Provides the percent of the cross-connect card VT matrix ports that are in use. Each port is one STS in size, and each can transport 28 VT1.5s. 24 VT matrix ports are available for the XCVT and XV10G cards.
- VT Matrix—(XCVT and XC10G) Provides the percent of the VT matrix resources that are in use. 672 are available, which is the number of VT matrix ports (24) multiplied by the number of VT1.5s in an STS (28).

Step 4 In the VT Matrix Port Detail section, you can view details of the VT Matrix Port usage:

- Drop—Identifies the source slot, port, and STS.
- Tunnel Name—VT tunnels use VT matrix ports on the tunnel source and destination nodes (VT tunnels do not use matrix resources on pass-through nodes). If the port is used by a VT tunnel, the tunnel name will appear here.
- % Used—Shows the percent of the matrix port that are in use. Each matrix port can carry 28 VT1.5s, so for example, if one STS carries seven VT1.5 circuits, the matrix port will be 25% used.
- Usage—Shows the port usage. For example, if one STS carries seven VT1.5 circuits, the matrix port will show that 7 of 28 are in use.

Step 5 As needed, you can perform the following actions:

- Click the **Refresh** button to see an updated XC Resources view. For example, if other users create circuits while you view the XC Resources tab, click **Refresh** to see the effects those circuits have on the VT matrix usage.
- Click the **Delete** button to delete STSs that use VT matrix resources but no longer carry VT circuits. This occasionally occurs when many VT circuits are added and deleted over a period of time. Stranded STSs appear as STSs with 0% usage in the VT Matrix Port Detail area. If stranded STSs appear, click the STS, then click **Delete** to free VT matrix capacity.

Note The Delete button requires a Superuser security level.

Note VT tunnels may appear as STSs with 0% capacity used. These cannot be deleted.

Stop. You have completed this procedure.

NTP-A151 Modify and Delete Circuits

Purpose	This procedure modifies and deletes ONS 15454 circuits and tunnels and DWDM optical channel network connections.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node containing the circuit that you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A230 Change a Circuit State" task on page 11-13.

Step 3 As needed, complete the "DLP-A231 Edit a Circuit Name" task on page 11-14.

Step 4 As needed, complete the "DLP-A232 Change Active and Standby Span Color" task on page 11-15.

Step 5 As needed, complete the "DLP-A233 Edit Path ProtectionCircuit Path Selectors" task on page 11-16.

Step 6 As needed, complete the "DLP-A263 Edit Path Protection Dual Ring Interconnect Circuit Hold-Off Timer" task on page 11-17.

Step 7 As needed, complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18.

Stop. You have completed this procedure.

DLP-A230 Change a Circuit State

Purpose	This task changes the state of a circuit. This task does not apply to DWDM-only nodes because optical channel network connections remain in the IS state.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit with the state that you want to change.

Note You cannot edit the circuit state if the circuit is routed to nodes with a CTC software release older than Release 3.4. These circuits will automatically be in service (IS).

Step 4 From the Tools menu, choose **Circuits > Set Circuit State**.

Step 5 In the Set Circuit State dialog box, choose the circuit state from the Target Circuit State drop-down menu:

- IS—Puts the circuit in service
- OOS—Puts the circuit out of service
- OOS-AINS—Puts the circuit out of service, auto in service
- OOS-MT—Puts the circuit out of service, maintenance

See Table 11-3 on page 11-5 for additional information about circuit states.

Step 6 If you want to apply the state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.

Step 7 Click **OK**.

> **Note** CTC will not change the state of the circuit source and destination port in certain circumstances. For example, if the circuit size is smaller than the port, such as a VT1.5 circuit on an STS port, CTC will not change the port state from IS to OOS. If CTC cannot change the port state, a message appears and you must change the port state manually.

Step 8 Return to your originating procedure (NTP).

DLP-A231 Edit a Circuit Name

Purpose	This task edits a circuit or DWDM optical channel network connection name.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to rename, then click **Edit**.

Step 4 In the General tab, click the **Name** field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters.

> **Note** If you will create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

Step 5 Click **Apply**.

Step 6 From File menu, choose **Close**.

Step 7 In the Circuits window, verify that the circuit was correctly renamed.

Step 8 Return to your originating procedure (NTP).

DLP-A232 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans shown on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple. This task does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in any view, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Circuit** tab.

Step 3 Complete one or more of the following steps, as required:

- To change the color of the active (working) span, go to Step 4.
- To change the color of the standby (protect) span, go to Step 5.
- To return active and standby spans to their default colors, go to Step 6.

Step 4 As needed, change the color of the active span:

a. Next to Active Span Color, click **Color**.

b. In the Pick a Color dialog box, click the color for the active span, or click **Reset** if you want the active span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, go to Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 5 As needed, change the color of the standby span:

a. Next to Standby Span Color, click **Color**.

b. In the Pick a Color dialog box, click the color for the standby span, or click **Reset** if you want the standby span to display the last applied (saved) color.

c. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 6 As needed, return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. In the Preferences dialog box, click the **Circuits** tab.

c. Click **Reset to Defaults**.

d. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 7 Return to your originating procedure (NTP).

DLP-A233 Edit Path ProtectionCircuit Path Selectors

Purpose	This task changes the path protection signal fail and signal degrade thresholds, the reversion and reversion time, and the PDI-P settings for one or more path protection circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 6-36 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

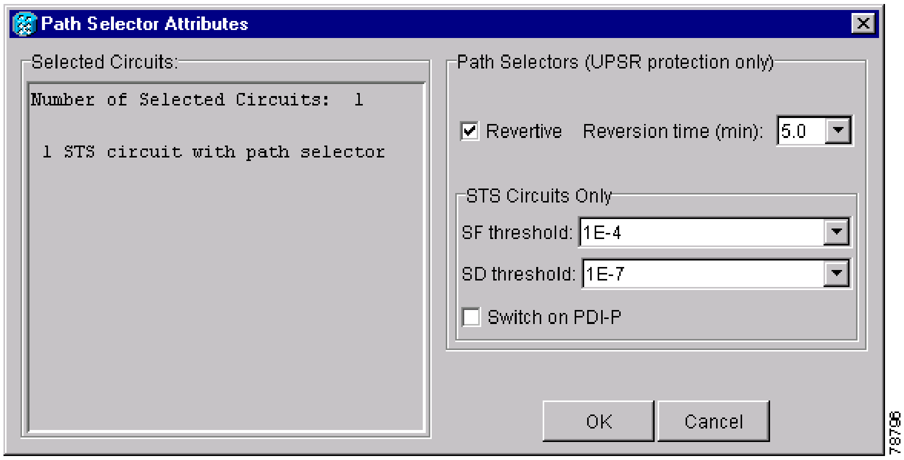
Step 3 In the Circuits tab, click the path protection circuit(s) you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose non-adjoining circuits) and click each circuit that you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Step 5 In the Path Selectors Attributes dialog box, edit the following path protection selectors, as needed (Figure 11-1):

- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If not checked, traffic does not revert.
- Reversion Time (Min)—If Revertive is checked, sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.
- SF Ber Level—Sets the path protection signal failure BER threshold (STS circuits only).
- SD Ber Level—Sets the path protection signal degrade BER threshold (STS circuits only).
- Switch on PDI-P—When checked, traffic switches if an STS payload defect indication is received (STS circuits only).

Figure 11-1 Editing Path Protection Path Selectors



Step 6 Click **OK** and verify that the changed values are correct in the Circuits window.

Step 7 Return to your originating procedure (NTP).

DLP-A263 Edit Path Protection Dual Ring Interconnect Circuit Hold-Off Timer

Purpose	This task changes the amount of time a path selector switch is delayed for circuits routed on a path protection dual ring interconnect (DRI) topology. Setting a switch hold-off time (HOT) prevents unnecessary back and forth switching when a circuit is routed through multiple path protection selectors.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 6-36 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Cisco recommends that you set the DRI port HOT value to zero and the circuit path selector HOT value to a number equal to or greater than zero.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 Click the path protection circuit you want to edit, then click **Edit**.

Step 4 In the Edit Circuit window, click the **UPSR Selectors** tab.

Step 5 Create a hold-off time for the circuit source and destination ports:

a. In the Holder Off Timer area, double-click the cell of the circuit source port (top row), then type the new hold-off time. The range is 0 to 10,000 ms in increments of 100.

b. In the Hold-Off Timer area, double-click the cell of the circuit destination port (bottom row), then type the hold-off time entered in Step a.

Step 6 Click **Apply**, then close the Edit Circuit window by choosing **Close** from the File menu.

Step 7 Return to your originating procedure (NTP).

DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections

Purpose	This task deletes circuits and DWDM optical channel network connections.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 2 Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.

Step 3 Investigate all network alarms and resolve any problems that may be affected by the circuit deletion. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab.

Step 6 Choose the circuits you want to delete, then click **Delete**.

Step 7 In the Delete Circuits confirmation dialog box, check one or both of the following, as needed:

- **Set drop ports to OOS**—(SONET circuits only.) Puts the circuit source and destination ports out of service if the circuit is the same size as the port or is the only circuit using the port. If the circuit is not the same size as the port or the only circuit using the port, CTC will not change the port state. This check box is not available if the circuit source or destination is on a TXP_MR_10G, MXP_2.5_10G, or TXP(P)_MR_2.5G card.
- **Notify when completed**—If checked, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are OOS and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, waiting for confirmation may take a few minutes. Circuits are deleted whether or not this check box is checked.

Note The CTC Alerts dialog box will not automatically open to show a deletion error unless you checked All alerts or Error alerts only in the CTC Alerts checkbox. For more information, see the "DLP-A327 Configure the CTC Alerts Dialog for Automatic Popup" task on page 3-30. If the CTC Alerts dialog is not set to open automatically with a notification, the red triangle inside the CTC Alerts toolbar icon indicates that a notification exists.

Step 8 Complete one of the following:

- If you checked "Notify when completed," the CTC Alerts dialog box appears. If you want to save the information, continue with Step 9. If you do not want to save the information, continue with Step 10.
- If you did not check "Notify when completed," the Circuits window appears. Continue with Step 11.

Step 9 If you want to save the information in the CTC Alerts dialog box, complete the following steps. If you do not want to save, continue with the next step.

a. Click **Save**.

b. Click **Browse** and navigate to the directory where you want to save the file.

c. Type the file name using a .txt file extension, and click **OK**.

Step 10 Click **Close** to close the CTC Alerts dialog box.

Step 11 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 12 Return to your originating procedure (NTP).

NTP-A278 Modify and Delete Overhead Circuits

Purpose	This procedure changes the tunnel type, repairs IP circuits, and deletes overhead circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 8, "Create Circuits and VT Tunnels."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting circuits can be service affecting and should be performed during a maintenance window.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 for a node on the network where you want to delete the circuit. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A332 Change Tunnel Type" task on page 11-20.

Step 3 As needed, complete the "DLP-A336 Repair an IP Tunnel" task on page 11-20.

Step 4 As needed, complete the "DLP-A334 Delete Overhead Circuits" task on page 11-21.

Stop. You have completed this procedure.

DLP-A332 Change Tunnel Type

Purpose	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional SDCC tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A313 Create a DCC Tunnel, page 8-93 DLP-A341 Create an IP-Encapsulated Tunnel, page 8-95
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the circuit tunnel that you want to convert.

Step 4 Click **Edit**.

Step 5 In the Edit circuit window, click the **Tunnel** tab.

Step 6 In the Attributes area, complete the following:

- If you are converting a traditional DCC tunnel to an IP-encapsulated tunnel, check the **Change to IP Tunnel** check box and type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10%).
- If you are converting an IP tunnel to a traditional DCC tunnel, check the **Change to SDCC Tunnel** check box.

Step 7 Click **Apply**.

Step 8 In the confirmation dialog box, click **Yes** to continue.

Step 9 In the Circuit Changed status box, click **OK** to acknowledge that the circuit change was successful.

Step 10 Return to your originating procedure (NTP).

DLP-A336 Repair an IP Tunnel

Purpose	This task repairs circuits that are in the INCOMPLETE state as a result of node IP address changes.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Obtain the original IP address of the node in question.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 From the Tools menu, choose **Overhead Circuits > Repair IP Circuits**.

Step 4 Review the text in the IP Repair wizard and click **Next**.

Step 5 In the Node IP address area, complete the following:

- Node—Choose the node that has an INCOMPLETE circuit.
- Old IP Address—Type the node's original IP address.

Step 6 Click **Next**.

Step 7 Click **Finish**.

Step 8 Return to your originating procedure (NTP).

DLP-A334 Delete Overhead Circuits

Purpose	This task deletes overhead circuits. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, the AIC and AIC-I card orderwire, and the AIC-I card user data channel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting overhead circuits is service affecting if the circuit ports are in service (IS). To put circuit ports out of service (OOS), see the "DLP-A214 Change the Service State for a Port" task on page 6-6.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click the overhead circuit that you want to delete: local or express orderwire, user data, IP-encapsulated tunnel, or DCC tunnel.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes** to continue.

Step 6 Return to your originating procedure (NTP).

NTP-A416 Convert a CTC Circuit to TL1 Cross-Connects

Purpose	This procedure converts CTC circuits to a set of TL1 cross-connects, which enables you to repair a missing cross-connect or change the cross-connect(s) using the TL1-like circuit option during circuit creation.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can only use this procedure with DS-1, DS-3, or OC-N circuits. You cannot use the procedure with VT tunnels, VT aggregation points, E-Series Ethernet card circuits, and DWDM optical channel network connections.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you want to convert the CTC circuits. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab, then choose the CTC circuit(s) that you want to convert to TL1 cross-connects. The circuit(s) must have an INCOMPLETE or ACTIVE status.

Step 4 From the Tools menu, choose **Circuits > Convert CTC Circuits to TL1 Cross Connects**.

Step 5 In the Convert to TL1 Cross Connect dialog box, click **Yes**.

The results of the conversion appear in the Convert to TL1 Cross Connect Results dialog box. If any circuits could not be converted, those circuits are listed.

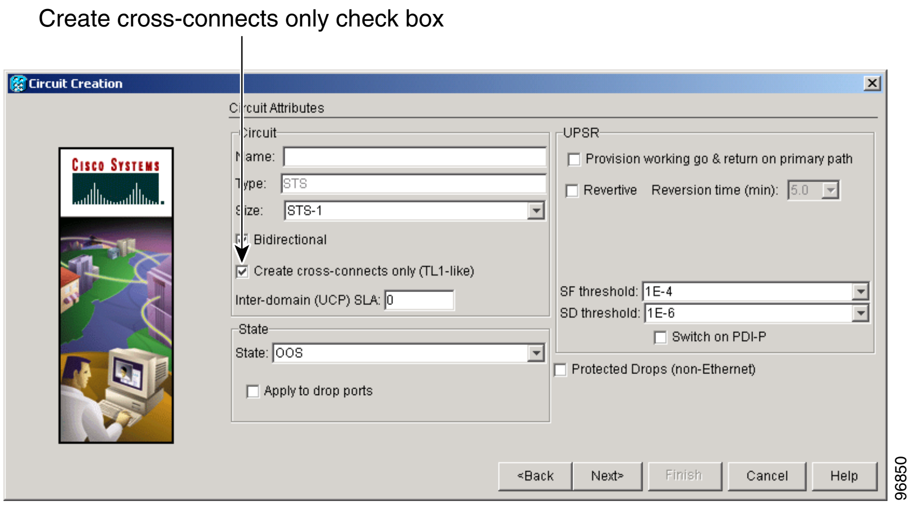
Step 6 In the Convert to TL1 Cross Connect Results dialog box, click **OK**.

If the circuit you selected had an INCOMPLETE status, its status will not change. If you selected an ACTIVE (complete) circuit, its status will change to UPGRADABLE.

Step 7 If you are repairing a circuit, complete the circuit creation procedure in Chapter 8, "Create Circuits and VT Tunnels," appropriate to the circuit you are repairing. On the Circuit Creation wizard, shown in Figure 11-2, check **Create cross-connects only (TL1-like)**.

After you repair or replace all missing cross-connects, CTC automatically merges them and the circuit status changes to UPGRADABLE.

Figure 11-2 Choosing the Cross-Connects Only Option



Step 8 To upgrade the repaired circuit to a CTC circuit, complete the "NTP-A417 Upgrade TL1 Cross-Connects to CTC Circuits" procedure on page 11-23.

Stop. You have completed this procedure.

NTP-A417 Upgrade TL1 Cross-Connects to CTC Circuits

Purpose	This procedure converts a series of cross-connects to an active CTC circuit. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	TL1-created or CTC-created TL1-like cross-connects must exist on the network.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you want to upgrade the TL1-created or CTC-created TL1-like cross-connects. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab, then choose one or more circuits with an UPGRADABLE status. These circuits contain a series of cross-connects that are linked together to form a circuit path. The cross-connects may have been created with TL1 or with CTC using the TL1-like cross-connects option.

Step 4 From the Tools menu, choose **Circuits > Upgrade TL1 Cross-Connects to CTC Circuits**.

Step 5 In the Upgrade Circuits dialog box, click **OK**.

The circuit status changes to ACTIVE.

Step 6 In the Circuit Upgrade Results dialog box, click **OK**.

Stop. You have completed this procedure.

NTP-A78 Create a Monitor Circuit

Purpose	This procedure creates a monitor circuit that monitors traffic on primary, bidirectional circuits. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	Bidirectional (two-way) circuits must exist on the network. See Chapter 8, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Monitor circuits cannot be used with EtherSwitch circuits.

Note For unidirectional circuits, create a drop to the port where the test equipment is attached.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you will create the monitor circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Choose the bidirectional (two-way) circuit that you want to monitor and click **Edit**.

Step 5 Verify that the circuit name is no longer than 44 characters. Monitor circuits append a "_MON" to the circuit name. If the name is longer than 44 characters, edit the name in the Name field, then click **Apply**.

Step 6 In the Edit Circuit window, click the **Monitors** tab.

The Monitors tab displays ports that you can use to monitor the circuit.

Note The Monitor tab is only available when the circuit has an ACTIVE status.

Step 7 On the Monitors tab, choose the monitor source port. The monitor circuit will display traffic coming into the node at the port you choose.

Note In Figure 11-3, you would choose either the DS1-14 card (to test circuit traffic entering Node 2 on the DS1-14) or the OC-N card at Node 1 (to test circuit traffic entering Node 1 on the OC-N card).

Step 8 Click **Create Monitor Circuit**.

Step 9 In the Circuit Destination section of the Circuit Creation wizard, choose the destination node, slot, port, STS, VT, or DS1 for the monitored circuit.

> **Note** In the Figure 11-3 example, the monitor circuit destination is Port 2 on the EC1-12 card.

Step 10 Click **Next**.

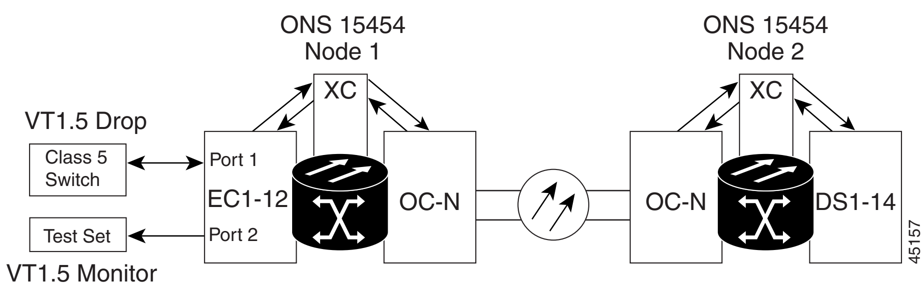
Step 11 In the Circuit Routing Preferences area, review the monitor circuit information. If you want the monitor circuit routed on a BLSR protection channel, click **Protection Channel Access**.

Step 12 Click **Finish**.

Step 13 In the Edit Circuit window, click **Close**. The new monitor circuit appears on the Circuits tab.

Figure 11-3 shows a sample monitor circuit setup. VT1.5 traffic is received by Port 1 of the EC1-12 card at Node 1. To monitor the VT1.5 traffic, test equipment is plugged into Port 2 of the EC1-12 card and a monitor circuit to Port 2 is provisioned in CTC. (Circuit monitors are one-way.) This example assumes circuits have been created.

Figure 11-3 VT1.5 Monitor Circuit Received at an EC1-12 Port



Stop. You have completed this procedure.

NTP-A79 Create a J1 Path Trace

Purpose	This procedure creates a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	ONS 15454 cards capable of transmitting and/or receiving path trace must be installed. See Table 11-4 on page 11-27 for a list of cards.
Prerequisite Procedures	Path trace can only be provisioned on OC-N (STS) circuits. See Chapter 8, "Create Circuits and VT Tunnels" for OC-N circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

> **Note** You cannot create a J1 path trace on a TL1-like circuit.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the network where you will create the path trace. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks as needed:

- As needed, complete the "DLP-A264 Provision Path Trace on Circuit Source and Destination Ports" task on page 11-26.
- As needed, complete the "DLP-A137 Provision Path Trace on OC-N Ports" task on page 11-30.

Stop. You have completed this procedure.

DLP-A264 Provision Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on STS circuit source ports and destination ports, or a VCAT circuit member. This task does not apply to DWDM-only nodes.
Tools/Equipment	ONS 15454 cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 11-4 on page 11-27 for a list of cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Circuits** tab.

Step 3 For the STS circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. See Table 11-4 for a list of cards.

Table 11-4 Path-Trace-Capable ONS 15454 Cards

J1 Function	Cards
Transmit and Receive	DS1-14[1]
	DS1N-14
	DS3-12E
	DS3N-12E
	DS3XM-6
	DS3i-N-12
	G1000-4
	M400T-12
	M4000-2
Receive Only	EC1-12
	OC3 IR 4/STM1 SH 1310
	OC3 IR 4/STM1 SH 1310-8
	OC12/STM4-4
	OC48 IR/STM16 SH AS 1310
	OC48 LR/STM16 LH AS 1550
	OC192 SR/STM64 IO 1310
	OC192 LR/STM64 LH 1550
	OC192 IR/STM SH 1550
	ML100T
	ML1000
	FC_MR-4

1. J1 path trace is not supported for DS-1s used in VT circuits.

Note For FC_MR-4 cards, the path trace string must be identical for all members of the VCAT circuit.

Note If neither port is on a transmit/receive card, you will not be able to complete this procedure. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 4 Choose the STS circuit you want to trace, then click **Edit**.

Step 5 If you chose a VCAT circuit, complete the following. If not, continue with Step 6.

a. In the Edit Circuit window, click the **Members** tab.

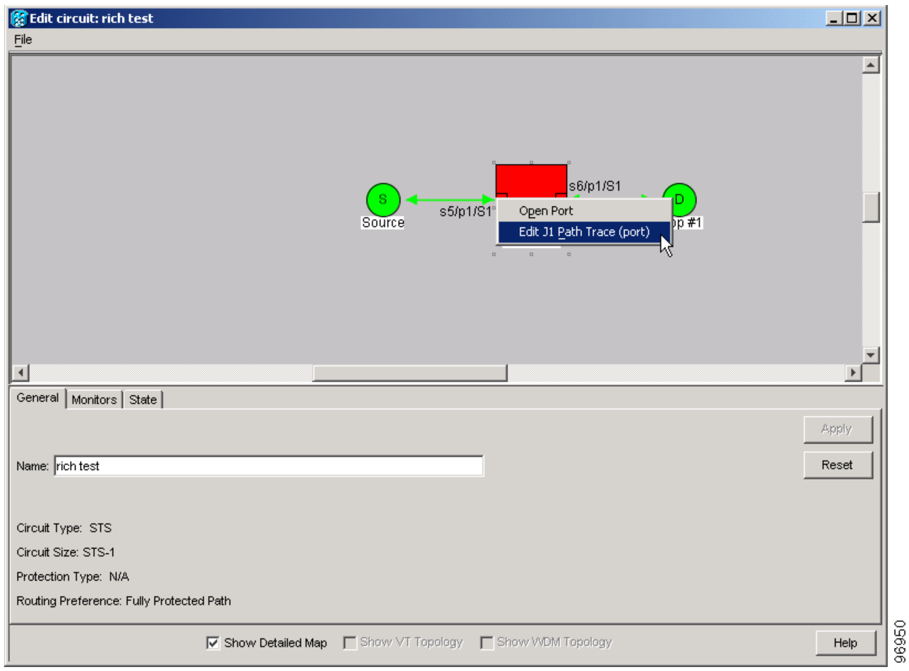
b. Click **Edit Member** and continue with Step 6.

Step 6 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.

Step 7 Provision the circuit source transmit string:

a. On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu. Figure 11-4 shows an example.

Figure 11-4 Selecting the Edit Path Trace Option



b. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**, then click **Close**.

Step 8 Provision the circuit destination transmit string:

a. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu (Figure 11-4).

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**.

Step 9 Provision the circuit destination expected string:

a. On the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.

- Manual—The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

c. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

d. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mismatch occurs.

e. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

Step 10 Provision the circuit source expected string:

a. In the Edit Circuit window (with Show Detailed Map chosen, see Figure 11-4 on page 11-28) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—Uses the first string received from the port at the other path trace end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set the Path Trace Mode field to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

e. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mismatch occurs.

f. Click **Apply**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit source expected string; the path trace process automatically determines the format.

Step 11 After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
- Click the **Reset** button to reread values from the port.

- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The expect and receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Step 12 Click **Close**.

The detailed circuit window indicates path trace with an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Step 13 Return to your originating procedure (NTP).

DLP-A137 Provision Path Trace on OC-N Ports

Purpose	This task monitors a path trace on OC-N ports within the circuit path.
Tools/Equipment	The OC-N ports you want to monitor must be on OC-N cards capable of receiving path trace. See Table 11-4 on page 11-27.
Prerequisite Procedures	DLP-A264 Provision Path Trace on Circuit Source and Destination Ports, page 11-26 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Other Node**. In the Select Node dialog box, choose the node where path trace was provisioned on the circuit source and destination ports.

Step 2 Click **Circuits**.

Step 3 Choose the STS circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 In the detailed circuit map right-click the circuit OC-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Note The OC-N port must be on a receive-only card listed in Table 11-4 on page 11-27. If not, the Edit Path Trace menu item will not appear.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—Uses the first string received from the port at the other path trace end as the current expected string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended because Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the OC-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close**.

Step 9 Return to your originating procedure (NTP).

Change Node Settings

This chapter explains how to modify node provisioning for the Cisco ONS 15454. To provision a new node, see Chapter 4, "Turn Up Node." To change default network element settings and to view a list of those settings, refer to the *Cisco ONS 15454 Release 4.6 Network Element Defaults* document.

> **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.

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A81 Change Node Management Information, page 12-2—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
2. NTP-A201 Change CTC Network Access, page 12-4—Complete this procedure as needed to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-A226 Modify DWDM Node Settings, page 12-7—Complete as needed.
4. NTP-A202 Customize the CTC Network View, page 12-10—As needed, complete this procedure to create domains and customize the appearance of the network map, including specifying a different default map, creating domains, selecting your own map or image, and changing the background color.
5. NTP-A203 Modify or Delete Card Protection Settings, page 12-15—Complete as needed.
6. NTP-A255 Delete Communications Channel Terminations, page 12-20—Complete this procedure as needed to delete DCC, LDCC, GCC, and DWDM OSC terminations.
7. NTP-A85 Change Node Timing, page 12-23—Complete as needed.
8. NTP-A205 Modify Users and Change Security, page 12-25—Complete this procedure as needed to make changes to user settings, including security level and security policies, and to delete users.
9. NTP-A87 Change SNMP Settings, page 12-33—Complete as needed.

NTP-A81 Change Node Management Information

Purpose	This procedure changes the node name, date, time, contact information, or the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A25 Set Up Name, Date, Time, and Contact Information, page 4-7
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 In the node view, click the **Provisioning > General** tabs.

Step 4 Complete the "DLP-A140 Change the Node Name, Date, Time, and Contact Information" task on page 12-2, as needed.

Step 5 Complete the "DLP-A265 Change the Login Legal Disclaimer" task on page 12-3, as needed.

Step 6 After confirming the changes, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A140 Change the Node Name, Date, Time, and Contact Information

Purpose	This procedure changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Changing the date, time, or time zone might invalidate the node's performance monitoring counters.

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude

- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click Reset Node Position.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time
- AIS-V Insertion On STS-1 Signal Degrade - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degrade - Path: SD-P BER

See the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-7 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-A265 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the following HTML commands to format the text, as needed:

- Begins boldface font
- Ends boldface font
- <center> Aligns type in the center of the window
- </center> Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- Ends the font size command
- <p> Creates a line break

- <sub> Begins subscript
- </sub> Ends subscript
- <sup> Begins superscript
- </sup> Ends superscript
- <u> Starts underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and formatting, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A201 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and OSPF options.
Tools/Equipment	None
Prerequisite Procedures	NTP-A169 Set Up CTC Network Access, page 4-9
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15454 networking information and procedures, including IP addressing examples, static route scenarios, Open Shortest Path First (OSPF) protocol, and routing information protocol options are provided in the IP Networking section of the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A266 Change IP Settings, page 12-5
- DLP-A142 Modify a Static Route, page 12-6
- DLP-A143 Delete a Static Route, page 12-6
- DLP-A144 Disable OSPF, page 12-7
- DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 4-16

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A266 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, DHCP access, firewall IIOP listener port, LCD IP display, and proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A249 Provision IP Settings, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution Changing the node IP address, subnet mask, or IIOP listener port causes the TCC2s to reboot. If Ethernet circuits using spanning tree protocol originate or terminate on E Series Ethernet cards installed in the node, circuit traffic will be lost for several minutes while the spanning trees reconverge. Other circuits are not affected by TCC2 reboots.

Step 1 In node view, click the **Provisioning** > **Network > General** tabs.

Step 2 Change any of the following:

- IP Address
- Suppress CTC IP Display
- LCD IP Setting
- Default Router
- Forward DHCP Request To
- MAC Address
- Net/Subnet Mask Length
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-A249 Provision IP Settings" task on page 4-10 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed a network field that will cause the node to reboot, such as the IP address, subnet mask or TCC CORBA Listener Port, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 15454 TCC2 cards will reboot, one at a time. A TCC2 card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

Step 5 Confirm that the changes appear on the Provisioning > Network > General tab. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

Step 6 Return to your originating procedure (NTP).

DLP-A142 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	DLP-A65 Create a Static Route, page 4-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab.

Step 3 Click the static route you want to edit.

Step 4 Click **Edit.**

Step 5 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-A65 Create a Static Route" task on page 4-15 for detailed field descriptions.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-A143 Delete a Static Route

Purpose	This task deletes an existing static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	DLP-A65 Create a Static Route, page 4-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-A144 Disable OSPF

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol process for an ONS 15454 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24 DLP-A250 Set Up or Change Open Shortest Path First Protocol, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN?** check box.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

NTP-A226 Modify DWDM Node Settings

Purpose	This procedure sets the network and node settings and provisions the node power levels on ONS 15454s that are provisioned for DWDM.
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	You must use Cisco MetroPlanner or another DWDM network calculation tool to prepare a configuration file for your network. NTP-A268 Install the DWDM or Hybrid Node Cards, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution DWDM settings are normally not changed at the individual node level. Any change to a DWDM node setting usually requires recalculation of power and attenuation levels at other nodes on the DWDM network. Do not change a DWDM node setting unless you are prepared to modify the settings of other DWDM nodes on the network.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Perform one of the following tasks as appropriate:

- DLP-A408 Modify DWDM Hub Node Settings, page 12-8.
- DLP-A409 Modify DWDM Terminal Node Settings, page 12-9.
- DLP-A410 Modify DWDM OADM Node Settings, page 12-9.
- DLP-A411 Modify DWDM Line Node Settings, page 12-10.

Step 3 Click the **Connections** tab, then click **Calculate Connections**.

Step 4 Verify that every connection matches the connections specified by the Cisco MetroPlanner design plan. If a connection is not correct:

a. Delete the connection. See the "DLP-A405 Delete a DWDM Connection" task on page 5-9.

b. Uninstall the fibers from the incorrect slot/unit/port.

c. Connect the fiber to the correct slot/unit/port.

d. Create a new connection. See the "DLP-A406 Create a DWDM Connection" task on page 5-8.

Step 5 Click the **Port Status** tab. Click **Launch ANS**.

ANS (Automatic Node Setup) automatically calculates variable optical attenuators (VOAs) set-points to match the expected channel profile at the amplifier input port.

Stop. **You have completed this procedure**.

DLP-A408 Modify DWDM Hub Node Settings

Purpose	This task modifies the node and network types and sets the channel power levels for a DWDM hub node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-2 on page 5-16.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A409 Modify DWDM Terminal Node Settings

Purpose	This task provisions the node and network types and power levels for a DWDM terminal node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-4 on page 5-18.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A410 Modify DWDM OADM Node Settings

Purpose	This task provisions the node and network types and power levels for a DWDM optical add/drop module (OADM) node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-5 on page 5-19.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-A411 Modify DWDM Line Node Settings

Purpose	This task modifies the node and network types for a DWDM line node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

Step 2 Complete the fields shown in Table 5-7 on page 5-22.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

NTP-A202 Customize the CTC Network View

Purpose	This procedure modifies the CTC network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- DLP-A145 Change the Network View Background Color, page 12-11
- DLP-A528 Change the Default Network View Background Map, page 12-11
- DLP-A268 Apply a Custom Network View Background Map, page 12-12
- DLP-A148 Create Domain Icons, page 12-13
- DLP-A149 Manage Domain Icons, page 12-14
- DLP-A269 Enable Dialog Box Do-Not-Display Option, page 12-15
- DLP-A498 Switch Between TDM and DWDM Network Views, page 12-13

Stop. You have completed this procedure.

DLP-A145 Change the Network View Background Color

Purpose	This task changes the network view background color or the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the View menu choose **Go to Network View**.

Step 2 If you want to change a domain background, double-click the domain. If not, continue with Step 3.

Step 3 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 4 In the Choose Color dialog box, select a background color.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A528 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu choose **Preferences > Map** and check the **Use Default Map** check box.

Step 2 In the node view, click the **Provisioning > Defaults** tabs.

Step 3 In the Defaults Selector area, choose **CTC** and then **network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down menu. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A268 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Step 1 From the Edit menu choose **Preferences > Map** and uncheck the **Use Default Map** check box

Step 2 From the View menu choose **Go to Network View**.

Step 3 Right-click the network or domain map and choose **Set Background Image**.

Step 4 Click **Browse**. Navigate to the graphic file you want to use as a background.

Step 5 Select the file. Click **Open**.

Step 6 Click **Apply** and then click **OK**.

Step 7 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15454 icons are visible.

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-A498 Switch Between TDM and DWDM Network Views

Purpose	Use this task to switch between TDM (Time Division Multiplexing) and DWDM (Dense Wavelength Division Multiplexing) network views. This task applies only to Release 4.6 or later.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 From the Network Scope drop-down menu on the toolbar, choose one of the following:

- All—displays both TDM and DWDM nodes
- TDM—displays only ONS 15454s with SONET or SDH cards including the transponder and muxponder cards.
- DWDM—displays only ONS 15454s with DWDM cards, including the transponder and muxponder cards.

Step 3 Return to your originating procedure (NTP).

DLP-A148 Create Domain Icons

Purpose	This task creates a domain, which is an icon that groups ONS 15454 icons in CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Domains created by one user are visible to all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-A149 Manage Domain Icons

Purpose	This task manages CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24 DLP-A148 Create Domain Icons, page 12-13
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Locate the domain action you want in Table 12-1 and complete the appropriate steps.

Table 12-1 Managing Domains

Domain action	Steps
Move a domain	Press Ctrl and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Choose **Move Node Back to Parent View**.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-A269 Enable Dialog Box Do-Not-Display Option

Purpose	This task ensures that a user-selected "Do not display" dialog box preference is enabled for subsequent sessions or it disables the do not display option.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 3-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box in a dialog box, the dialog box is not displayed for any other users who perform that operation on the network from the same computer unless the command is overridden using the following task. (The preference is stored on the computer, not in the node database.)

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" is enabled.

Step 3 Choose one of the following options, or uncheck the individual dialog boxes that you want to appear:

- **Don't Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

NTP-A203 Modify or Delete Card Protection Settings

Purpose	This procedure modifies and deletes card protection settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A170 Create Protection Groups, page 4-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Modifying and deleting protection groups can be service affecting.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A150 Modify a 1:1 Protection Group, page 12-16
- DLP-A152 Modify a 1:N Protection Group, page 12-17
- DLP-A154 Modify a 1+1 Protection Group, page 12-18
- DLP-A270 Modify a Y Cable Protection Group, page 12-18
- DLP-A499 Modify a Splitter Protection Group, page 12-19
- DLP-A155 Delete a Protection Group, page 12-20

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A150 Modify a 1:1 Protection Group

Purpose	This task modifies a 1:1 protection group for electrical (DS-1, DS-3, EC-1, and DS3XM-6) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A71 Create a 1:1 Protection Group, page 4-28
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1:1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 13-63.

Step 5 Return to your originating procedure (NTP).

DLP-A152 Modify a 1:N Protection Group

Purpose	This task modifies a 1:N protection group for DS-1 and DS-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A72 Create a 1:N Protection Group, page 4-29 DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the DS-1 and DS-3 cards are installed according to the 1:N specifications in the "DLP-A72 Create a 1:N Protection Group" task on page 4-29.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

Step 3 In the Protection Groups area, click the 1:N protection group you want to modify.

Step 4 In the Selected Group area, change any of the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Available Entities—If cards are available, they will appear here. Use the arrow buttons to move them into the Working Cards column.
- Working Entities—Use the arrow buttons to move cards out of the Working Cards column.
- Reversion Time—Choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A72 Create a 1:N Protection Group" task on page 4-29 for field descriptions.

Step 5 Click **Apply**. The changes are applied. Confirm that the changes appear; if not repeat the task.

Note To convert electrical protection groups, see the "NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 13-63.

Step 6 Return to your originating procedure (NTP).

DLP-A154 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port (OC-3, OC-12, OC-12 IR, OC-48, OC-48AS, and OC-192).
Tools/Equipment	None
Prerequisite Procedures	DLP-A73 Create a 1+1 Protection Group, page 4-30
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the 1+1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—Check or uncheck
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A270 Modify a Y Cable Protection Group

Purpose	This task modifies a Y cable protection group for any client port on a MXP_2.5G_10G, TXP_MR_2.5G, or TXP_MR_10G card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A252 Create a Y-Cable Protection Group, page 4-32
	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the Y Cable protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "DLP-A252 Create a Y-Cable Protection Group" task on page 4-32 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A499 Modify a Splitter Protection Group

Purpose	This task modifies a Splitter protection group for any client port on a TXPP_MR_2.5G card. Splitter protection is automatically created when the TXPP transponder card is installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the Splitter protection group that you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A155 Delete a Protection Group

Purpose	This task deletes a 1:1, 1:N, 1+1, or Y Cable protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups area, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box. Confirm that the changes appear; if they do not, repeat Steps 1 through 3.

Step 5 Return to your originating procedure (NTP).

NTP-A255 Delete Communications Channel Terminations

Purpose	This procedure deletes a DCC, LDCC, GCC, and DWDM OSC terminations on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A354 Provision SONET DCC Terminations, page 6-4 or DLP-A355 Provision SONET LDCC Terminations, page 6-5 or DLP-A343 Provision GCC Terminations, page 7-4 or DLP-A342 Provision OSC Terminations, page 5-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Provisioning > DCC/GCC/OSC** tabs.

Step 3 As needed, complete the following tasks:

- DLP-A156 Delete a SONET DCC Termination, page 12-21
- DLP-A359 Delete a SONET LDCC Termination, page 12-21

- DLP-A360 Delete a GCC Termination, page 12-22
- DLP-A361 Delete a DWDM OSC Termination, page 12-22

Stop. You have completed this procedure.

DLP-A156 Delete a SONET DCC Termination

Purpose	This task deletes a SONET DCC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **DCC** tab.

Step 2 Click the DCC termination to be deleted and click **Delete**. The Delete SDCC Termination dialog box appears.

Step 3 Check the **Set Port Out of Service** check box if you want to change the port state to out of service (this may be service affecting).

Step 4 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A359 Delete a SONET LDCC Termination

Purpose	This task deletes a SONET LDCC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Click the **LDCC** tab.

Step 2 Click the LDCC termination to be deleted and click **Delete**. The Delete LDCC Termination dialog box appears.

Step 3 Check the **Set Port Out of Service** check box if you want to change the port state to out of service (this may be service affecting).

Step 4 Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-A360 Delete a GCC Termination

Purpose	This task deletes the DWDM GCC terminations required for network setup when using the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **GCC** tab.

Step 2 In the GCC Terminations pane, click **Delete.**

Step 3 In the Delete GCC Terminations dialog box, check **Set port OOS** checkbox if you want to place ports out of service.

Step 4 Click **Yes**. GCC-EOC alarms appear until all network GCC terminations are deleted and the ports are out of service.

Step 5 Return to your originating procedure (NTP).

DLP-A361 Delete a DWDM OSC Termination

Purpose	This task deletes a DWDM OSC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Deleting a OSC termination may cause node isolation and loss of visibility to nodes that do not have other OSCs or network connections to the CTC computer.

Step 1 Click the **OSC** tab.

Step 2 Click the OSC termination you want to delete and click **Delete**.

Step 3 In the Delete OSC Termination confirmation box, click **Yes**. Confirm that the changes appear; of not, repeat the task.

Until all network OSC terminations are deleted, LOS or power failure alarms on the OPT-BST, OSCM, and OSC-CSM might appear.

Step 4 Return to your originating procedure (NTP).

NTP-A85 Change Node Timing

Purpose	This procedure changes the SONET timing settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 As needed, complete the "DLP-A157 Change the Node Timing Source" task on page 12-23.

Step 4 If you need to change any internal timing settings, follow the "DLP-A70 Set Up Internal Timing" task on page 4-25 for the settings you need to modify.

Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 5 If you need to verify timing after removing a node from a BLSR or path protection, see the "DLP-A195 Verify Timing in a Reduced Ring" task on page 16-11.

Step 6 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A157 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15454
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following procedure may be service affecting and should be performed during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing section, change any of the following information:

- Timing Mode

  Note Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Revertive Time

See the "DLP-A69 Set Up External or Line Timing" task on page 4-23 for field descriptions.

Step 3 In the BITS Facilities section, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State
- BITS Out State
- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

Step 4 In the Reference Lists area, you can change the following information:

Note Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference
- BITS 1 Out
- BITS 2 Out

Step 5 Click **Apply**. Confirm that the changes appear; of not, repeat the task.

Step 6 Return to your originating procedure (NTP).

NTP-A205 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A30 Create Users and Assign Security, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A271 Change Security Policy—Single Node, page 12-25
- DLP-A272 Change Security Policy—Multiple Nodes, page 12-27
- DLP-A511 Change Node Access and PM Clearing Privilege, page 12-28
- DLP-A158 Change User Password and Security Level—Single Node, page 12-29
- DLP-A160 Change User Password and Security Level—Multiple Nodes, page 12-29
- DLP-A159 Delete User—Single Node, page 12-31
- DLP-A161 Delete User—Multiple Nodes, page 12-32

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A271 Change Security Policy—Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Policy** tabs.

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 4 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 5 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change their password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- Single Session Per User—If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 7 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-A272 Change Security Policy—Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Policy** tabs. A read-only table of nodes and their policies appears.

Step 3 Click a node on the table that you want to modify, then click **Change**.

Step 4 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 5 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 6 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 7 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change their password for each security level. The range is 2 to 20 days.

Step 8 In the Other area, you can provision the following:

- Single Session Per User—If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 9 In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.

Step 10 Click **OK**.

Step 11 In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.

Step 12 Return to your originating procedure (NTP).

DLP-A511 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security > Access** tabs.

Step 2 In the Access area, provision the following:

- LAN access—Sets the access paths to the node:
  - No LAN Access—Allows access to the node only through DCC connections. Access through the TCC2 RJ-45 port and backplane is not permitted.
  - Backplane only—Allows access through DCC connections and the backplane. Access through the TCC2 RJ-45 port is not allowed.
  - Front and Backplane—Allows access through DCC, TCC2 RJ-45 and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and “DCC only” is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.

Step 3 In the Shell Access area, set the shell program used to access the node:

- Telnet—If chosen, allows access to the node using Telnet. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). If chosen, choose the Telnet port. Port 23 is the default.
- SSH—If chosen, allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links. If chosen, Port 22 is the default port. It cannot be changed.

Step 4 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: RETRIEVE, PROVISIONING, MAINTENANCE, or SUPERUSER.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A158 Change User Password and Security Level—Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Click the user whose settings you want to modify, then click **Change**.

Step 3 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out the user

See the "NTP-A30 Create Users and Assign Security" procedure on page 4-4 for field descriptions.

Step 4 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 5 Return to your originating procedure (NTP).

DLP-A160 Change User Password and Security Level—Multiple Nodes

Purpose	This task changes settings for an existing user at multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note You must add the same user name and password to each node the user will access.

Step 1 From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.

Step 2 Click the **Provisioning** > **Security** > **Users** tabs. Highlight the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, you can:

- Change a user's password
- Modify the user's security level
- Lock out the user

See the "DLP-A75 Create a New User—Multiple Nodes" task on page 4-5 for field descriptions.

Step 5 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**. A Change Results confirmation dialog box appears.

Step 7 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-A315 Log Out a User—Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security > Active Logins** tabs.

Step 2 Choose the user that you want to log out and click **Logout**.

Step 3 In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out. This prevents the user from logging in after logout based on parameters provided in the user lockouts in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy—Single Node" task on page 12-25 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-A316 Log Out a User—Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 From the view menu, chose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** > **Active Logins** tabs.

Step 3 Choose the user you want to log out.

Step 4 Click **Logout**.

Step 5 In the Logout User dialog box, check the nodes where you want to log out the user.

Step 6 Check **Lockout before Logout** if you want to lock the user out prior to logout. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-A271 Change Security Policy—Single Node" task on page 12-25 for more information.

Step 7 In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 8 Click **OK**.

Step 9 Return to your originating procedure (NTP).

DLP-A159 Delete User—Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A315 Log Out a User—Single Node" task on page 12-30, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, verify that the user name displayed is the one you want to delete. Click **Logout before delete? if the user is currently logged in. (You cannot delete users if they are logged in.)**

Step 5 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 6 Return to your originating procedure (NTP).

DLP-A161 Delete User—Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-A316 Log Out a User—Multiple Nodes" task on page 12-31, or you can choose the "Logout before delete" option in the Delete User dialog box.

Note CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** tabs. Highlight the name of the user you want to delete.

Step 3 Click **Delete**. The Delete User dialog box appears.

Step 4 In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.

Step 5 Click **OK**. A User Deletion Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 7 Return to your originating procedure (NTP).

NTP-A87 Change SNMP Settings

Purpose	This procedure modifies SNMP settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-A256 Set Up SNMP, page 4-33
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A273 Modify SNMP Trap Destinations, page 12-33
- DLP-A163 Delete SNMP Trap Destinations, page 12-34

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A273 Modify SNMP Trap Destinations

Purpose	This task modifies the SNMP trap destinations on an ONS 15454 including community name, default UDP port, SNMP trap version, and maximum traps per second.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Select a trap from the **Trap Destinations** dialog box.

For a description of SNMP traps, refer to the *Cisco ONS 15454 Reference Manual*.

Step 3 Type the SNMP community name in the Community Name field.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system.

Note The default UDP port for SNMP is 162.

Step 4 Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

Step 5 Set your maximum traps per second in the Max Traps per Second field.

Note The Max Traps per Second is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, there is no maximum and all traps are sent.

Step 6 If you want to allow the ONS 15454 SNMP agent to accept SNMP SET requests on certain MIBs, check the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 Click **Apply**.

Step 8 SNMP settings are now configured. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen. Confirm that the changes appear; if not repeat the task.

Step 9 Return to your originating procedure (NTP).

DLP-A163 Delete SNMP Trap Destinations

Purpose	This task deletes SNMP trap destinations on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 In the Trap Destinations area, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

Change Card Settings

This chapter explains how to change line and threshold settings on Cisco ONS 15454 cards.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

Caution Changing card settings can be service affecting. You should make all changes during a scheduled maintenance window.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards, page 13-2—As needed, complete this procedure to change line and threshold settings for all electrical cards (EC-1, DS-1, DS-3, DS3i-N-12, and DS3MX-6).
2. NTP-A89 Modify Line Settings and PM Parameter Thresholds for OC-N Cards, page 13-23—As needed, complete this procedure to change line and threshold settings for all optical (OC-N) cards.
3. NTP-A206 Modify Line Settings and PM Parameter Thresholds for TXP_MR_10G Cards, page 13-28—As needed, complete this procedure to change line and threshold settings for TXP_MR_10G (transponder) cards.
4. NTP-A207 Modify Line Settings and PM Parameter Thresholds for MXP_2.5G_10G Cards, page 13-37—As needed, complete this procedure to change line and threshold settings for MXP_2.5G_10G (muxponder) cards.
5. NTP-A237 Modify Line Settings and PM Parameter Thresholds for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-46—As needed, complete this procedure to change line and threshold settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
6. NTP-A90 Modify Alarm Interface Controller Settings, page 13-57—As needed, complete this procedure to change external alarms and controls (environmental alarms) and/or orderwire settings.
7. NTP-A118 Modify Alarm Interface Controller-International Settings, page 13-60—As needed, complete this procedure to change external alarms and controls and/or orderwire settings.
8. NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection, page 13-63—As needed, complete this procedure to change the protection type on DS-1 or DS-3 cards.
9. NTP-A229 Modify Line Settings and PM Parameter Thresholds for Optical Service Channel Cards, page 13-68—As needed, complete this procedure to change the optical service channel card settings.

10. NTP-A230 Modify Line Settings and PM Parameter Thresholds for Amplifier Cards, page 13-74—As needed, complete this procedure to change the amplifier card settings.
11. NTP-A231 Modify Line Settings and PM Parameter Thresholds for Multiplexer and Demultiplexer Cards, page 13-79—As needed, complete this procedure to change the multiplexer and demultiplexer card settings.
12. NTP-A259 Modify Line Settings and PM Parameter Thresholds for FC_MR-4 Cards, page 13-84—As needed, complete this procedure to change FC_MR-4 card port and threshold settings.

NTP-A88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards

Purpose	This procedure changes the line and threshold settings for electrical cards. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the electrical card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7 to preserve the existing database.

Step 3 Perform any of the following tasks as needed:

- DLP-A165 Change Line and Threshold Settings for the DS1-14 or DS1N-14 Cards, page 13-3
- DLP-A166 Change Line and Threshold Settings for the DS3-12 or DS3N-12 Cards, page 13-6
- DLP-A167 Change Line and Threshold Settings for the DS3E-12 or DS3N-12E Cards, page 13-9
- DLP-A168 Change Line and Threshold Settings for the DS3XM-6 Card, page 13-13
- DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards, page 13-17
- DLP-A169 Change Line and Threshold Settings for the EC1-12 Card, page 13-20

Step 4 When you are finished changing the card settings, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A165 Change Line and Threshold Settings for the DS1-14 or DS1N-14 Cards

Purpose	This task changes the line and threshold settings for the DS1-14 or DS1N-14 (DS-1) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the DS1-14 or DS1N-14 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds, or SONET Thresholds** tab.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-1. For definitions of the Line Threshold settings, see Table 13-2. For definitions of the Electrical Path Threshold settings, see Table 13-3. For definitions of the SONET Threshold settings, see Table 13-4.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 13-1 describes the values on the Provisioning > Line tabs for the DS-1 cards.

Table 13-1 Line Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port #	Sets the port number.	1 to 14 (read-only)
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 13-1 Line Options for DS1-14 and DS1N-14 Cards (continued)

Parameter	Description	Options
Line Type	Defines the line framing type.	• D4 • ESF - Extended Super Frame • Unframed
Line Coding	Defines the DS-1 transmission coding type.	• AMI - Alternate Mark Inversion (default) • B8ZS - Bipolar 8 Zero Substitution
Line Length	Defines the distance (in feet) from the backplane connection to the next termination point.	• 0 - 131 • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, in 15-minute increments

Table 13-2 describes the values on the Provisioning > Line Thresholds tabs for the DS-1 cards.

Table 13-2 Line Thresholds Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port	Port number	1 to 14 (read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-3 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS-1 cards.

Table 13-3 Electrical Path Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port	Port number	1 to 14 (read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
SAS	Severely errored frame/alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
AISS	Alarm indication signal seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-4 describes the values on the Provisioning > SONET Thresholds tabs for the DS-1 cards.

Table 13-4 SONET Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port	DS-1 ports partitioned for STS	Read-only Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near End, STS termination).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near End, STS termination).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near End, STS termination).

Table 13-4 SONET Threshold Options for DS1-14 and DS1N-14 Cards (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near End, STS termination).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near End, STS termination).

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A166 Change Line and Threshold Settings for the DS3-12 or DS3N-12 Cards

Purpose	This task changes the line and threshold settings for the DS3-12 or DS3N-12 (DS-3) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the DS3-12 or DS3N-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** tab.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-5. For definitions of the Line Threshold settings, see Table 13-6. For definitions of the Elect Path Threshold settings, see Table 13-7 on page 13-8. For definitions of the SONET Threshold settings, see Table 13-8 on page 13-9.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 13-5 describes the values on the Provisioning > Line tabs for the DS-3 cards.

Table 13-5 Line Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port #	Sets the port number.	1 to 12
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically 0 to 48 hours, 15-minute increments

Table 13-6 describes the values on the Provisioning > Line Thresholds tabs for the DS-3 cards.

Table 13-6 Line Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port	Port number	1 to 12
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-6 Line Threshold Options for DS3-12 or DS3N-12 Cards (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-7 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS-3 cards.

Table 13-7 Electrical Path Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port	Port number	1 to 12 (read-only)
EB	Errored blocks	Numeric. Can be set for 15-minute or one-day intervals, near end or far end. Select the bullet and click **Show Thresholds**.
BBE	Background block errors	Numeric. Can be set for 15-minute or one-day intervals, near end or far end. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals, near end or far end. Select the bullet and click **Show Thresholds**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals, near end or far end. Select the bullet and click **Show Thresholds**.
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals, near end or far end. Select the bullet and click **Show Thresholds**.
AISS	Alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

Table 13-8 describes the values on the Provisioning > SONET Thresholds tabs for the DS-3 cards.

Table 13-8 SONET Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port	DS-3 ports partitioned for STS	Read-only Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A167 Change Line and Threshold Settings for the DS3E-12 or DS3N-12E Cards

Purpose	This task changes the line and threshold settings for the DS3E-12 or DS3N-12E (DS3E) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the DS3E is installed in an ONS 15454 slot that is provisioned for a DS-3 card, the DS3E enhanced performance monitoring parameters are unavailable. If this occurs, remove the DS3E from the ONS 15454, delete the DS-3 card in Cisco Transport Controller (CTC) using the "DLP-A191 Delete a Card" task on page 2-58, and provision the slot for the DS3E using the "DLP-A330 Preprovision a Slot" task on page 5-5.

Step 1 Double-click the DS3E-12 or DS3N-12E card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds**, or **SONET Thresholds** tab.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-9. For definitions of the Line Threshold settings, see Table 13-10. For definitions of the Electrical Path Thresholds, see Table 13-11. For definitions of the SONET Threshold settings, see Table 13-12.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 13-9 describes the values on the Provisioning > Line tabs for the DS3E cards.

Table 13-9 Line Options for the DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port #	Sets the port number.	1 to 12 (Read-only)
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• M13 • C Bit • Auto Provisioned
Detected Line Type	Displays the detected line type.	Read-only

Table 13-9 Line Options for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Description	Options
Line Coding	Defines the DS3E transmission coding type.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 13-10 describes the values on the Provisioning > Line Thresholds tabs for the DS3E cards.

Table 13-10 Line Threshold Options for the DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port	1 to 12 (Read-only)	Port number
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-11 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3E cards.

Table 13-11 Electrical Path Options for the DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port	1 to 12 (Read-only)	Port number
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

Table 13-11 Electrical Path Options for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Description	Options
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SAS	Severely errored frame/alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
AIS	Alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

Table 13-12 describes the values on the Provisioning > SONET Thresholds tabs for the DS3E cards.

Table 13-12 SONET Threshold Options for DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port	DS-3 ports partitioned for STS	Read-only Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).

Table 13-12 SONET Threshold Options for DS3-12E and DS3N-12E Cards (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, STS termination only).

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A168 Change Line and Threshold Settings for the DS3XM-6 Card

Purpose	This task changes the line and threshold settings for the DS3XM-6 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The DS3XM-6 (transmux) card can accept up to six channelized DS-3 signals and convert each signal to 28 VT1.5 signals. Conversely, the card can take 28 T-1s and multiplex them into a channeled C-bit or M13 framed DS-3.

Step 1 In node view, double-click the DS3XM-6 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** tab.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-13. For definitions of the Line Threshold settings, see Table 13-14. For definitions of the Electrical Path Thresholds, see Table 13-15. For definitions of the SONET Threshold settings, see Table 13-16.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 13-13 describes the values on the Provisioning > Line tabs for the DS3XM-6 cards.

Table 13-13 Line Options for the DS3XM-6 Parameters

Parameter	Description	Options
Port #	Sets the port number.	1 to 6 (read-only)
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Line Type	Defines the line framing type.	• M13 - default • C BIT
Line Coding	Defines the DS-1 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 13-14 lists the line threshold options for DS3XM-6 cards.

Table 13-14 Line Threshold Options for the DS3XM-6 Card

Parameter	Description	Options
Port	Port number	1 to 6 (read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
LOSS	Loss of signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.

Table 13-15 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3XM-6 cards.

Table 13-15 Electrical Path Threshold Options for the DS3XM-6 Card

Parameter	Description	Options
Port	Port number	1 to 6 (read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).
SAS	Severely errored frame/alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).

Table 13-15 Electrical Path Threshold Options for the DS3XM-6 Card (continued)

Parameter	Description	Options
AISS	Alarm indication signal seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).

Table 13-16 describes the values on the Provisioning > SONET Thresholds tabs for the DS3XM-6 cards.

Table 13-16 SONET Threshold Options for the DS3XM-6 Card

Parameter	Description	Options
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A526 Change Line and Threshold Settings for the DS3i-N-12 Cards

Purpose	This task changes the line and threshold settings for the DS3i-N-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the DS3i-N-12 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, Line Thresholds, Elect Path Thresholds,** or **SONET Thresholds** subtab.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-9. For definitions of the Line Threshold settings, see Table 13-10. For definitions of the Electrical Path Thresholds, see Table 13-11. For definitions of the SONET Threshold settings, see Table 13-12.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Table 13-17 describes the values on the Provisioning > Line tabs for the DS3i-N-12 cards.

Table 13-17 Line Options for the DS3i-N-12 Cards

Parameter	Description	Options
Port #	Sets the port number.	1 to 12 (Read-only)
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 13-17 Line Options for the DS3i-N-12 Cards (continued)

Parameter	Description	Options
Line Type	Defines the line framing type.	• Unframed • M13 • C Bit • Auto Provisioned
Detected Line Type	Displays the detected line type.	Read-only
Line Coding	Defines the DS3E transmission coding type.	B3ZS (Read-only)
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	• 0 - 225 (default) • 226 - 450
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 13-18 describes the values on the Provisioning > Line Thresholds tabs for the DS3i-N-12 cards.

Table 13-18 Line Threshold Options for the DS3i-N-12 Cards

Parameter	Description	Options
Port	Port number	1 to 12 (Read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.

Table 13-19 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3i-N-12 cards.

Table 13-19 Electrical Path Options for the DS3i-N-12 Cards

Parameter	Description	Options
Port	Port number	1 to 12 (Read-only)
CVP	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
ESP	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SESP	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
SASP	Severely errored frame/alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
UASP	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
AISSP	Alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

Table 13-20 describes the values on the Provisioning > SONET Thresholds tabs for the DS3i-N-12 cards.

Table 13-20 SONET Threshold Options for DS3i-N-12 Cards

Parameter	Description	Options
Port	Port number	1 to 12 (Read-only)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the **Show Thresholds** button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds**.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (STS and VT Term).

Table 13-20 SONET Threshold Options for DS3i-N-12 Cards (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Show Thresholds** (Near and Far End, Sts Term or Vt Term).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click **Show Thresholds**.

Note The threshold value appears after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-A169 Change Line and Threshold Settings for the EC1-12 Card

Purpose	This task changes the line and threshold settings for the EC1-12 (EC-1) card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the EC-1 card where you want to change the line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line, SONET Thresholds,** or **SONET STS** tabs.

Note See Chapter 9, "Manage Alarms" for information about the Alarm Behavior tab.

Step 4 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 13-21. For definitions of the SONET Threshold settings, see Table 13-22.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

Note The STS subtab is used to provision intermediate path performance monitoring (IPPM). To provision IPPM, circuits must be provisioned on the EC1-12 card. For circuit creation procedures, go to Chapter 8, "Create Circuits and VT Tunnels." To provision IPPM, go to the "DLP-A121 Enable/Disable Pointer Justification Count Performance Monitoring" task on page 10-27.

Table 13-21 describes the values on the Line tab for the EC1-12 card.

Table 13-21 Line Options for the EC1-12 Card

Parameter	Description	Options
Port #	Displays the EC-1 card port number.	1 to 12 (read-only)
Port Name	Sets a name for the port (optional).	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
PJStsMon#	Sets the STS that will be used for pointer justification; if set to zero, no STS is used.	• 0 (default) • 1
Line Buildout	Defines the distance (in feet) from backplane to next termination point.	• 0 - 225 (default) • 226 - 450
Rx Equalization	For early EC1-12 card versions, equalization can be turned off if the line length is short or the environment is extremely cold; Rx Equalization should normally be set to On.	• On (checked, default) • Off (unchecked)
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments

Table 13-22 lists the SONET Threshold options for EC1-12 cards.

Table 13-22 SONET Threshold Options for the EC1-12 Card

SONET Layer	Parameter	Description	Options
All	Port #	EC-1 card port #	1 to 12 (read-only)
Line (L)	CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
Line (L)	SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
Section (S)	CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh** (Near End only).
	ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	SEFS	Severely errored framing seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.

Table 13-22 SONET Threshold Options for the EC1-12 Card (continued)

SONET Layer	Parameter	Description	Options
Path (P)	CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh** (Near and Far End).
	ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.
	UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click **Refresh**.

Step 7 Return to your originating procedure (NTP).

NTP-A89 Modify Line Settings and PM Parameter Thresholds for OC-N Cards

Purpose	This procedure changes the line and threshold settings for optical cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A16 Install the OC-N Cards, page 2-12
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the OC-N card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A170 Change Line Transmission Settings for OC-N Cards, page 13-24
- DLP-A171 Change Threshold Settings for OC-N Cards, page 13-26
- DLP-A172 Change an Optical Port to SDH, page 13-28

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A170 Change Line Transmission Settings for OC-N Cards

Purpose	This task changes the line transmission settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to change the line settings.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Modify any of the settings described in Table 13-23.

Note The STS subtab is used to provision IPPM. To provision IPPM, circuits must be provisioned on the EC1-12 card.

Table 13-23 OC-N Card Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	• 1 (OC-12, OC-48, OC-192) • 1-4 (OC-3, OC12-4)
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference.	• Yes • No (Read-only)

Table 13-23 OC-N Card Line Settings (continued)

Parameter	Description	Options
Enable Synch Messages	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes • No
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte.	• Yes • No
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port.	• 0 - 3 (OC-3, per port) • 0 - 12 (OC-12) • 0 - 48 (OC-48) • 0 - 192 (OC-192)
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
Type	Defines the port as SONET or SDH. The Enable Sync Msg field and the Send Do Not Use field must be disabled before the port can be set to SDH.	• Sonet • SDH
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A171 Change Threshold Settings for OC-N Cards

Purpose	This task changes threshold settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to change the threshold settings.

Step 2 Click the **Provisioning > SONET Thresholds** tabs.

Step 3 Modify any of the settings found in Table 13-24.

Table 13-24 OC-N Threshold Options

Parameter	Description	Options
Port	Port number	• 1 (OC-12, OC-48, OC-192) • 1-4 (OC-3, OC12-4)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
SEFS	Severely errored framing seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click **Refresh**.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals for Line. Select the bullet and click **Refresh** or Path (Near and Far End)
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click **Refresh**.
PSC	Protection Switching Count (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.

Table 13-24 OC-N Threshold Options (continued)

Parameter	Description	Options
PSD	Protection Switch Duration (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSC-W	Protection Switching Count - Working line bidirectional line switch rings (BLSRs) are not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R performance monitoring parameters (PMs) do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSD-W	Protection Switching Duration - Working line BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSC-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSD-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSC-R	Protection Switching Count - Ring BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.
PSD-R	Protection Switching Duration - Ring BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A172 Change an Optical Port to SDH

Purpose	This task provisions a port on an OC-N card for SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to provision a port for SDH.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 In the Type field for the desired port, choose **SDH**.

Note Before you can change the port type to SDH, ensure the following: the EnableSyncMsg and SendDoNotUse fields are unchecked, the card is not part of a BLSR or 1+1 protection group, the card is not part of an orderwire channel, and the card is not a SONET data communications channel/generic communications channel (DCC/GCC) termination point.

Step 4 Click **Apply**.

Step 5 If the card is a multiport OC-N card, for example a four-port OC-3, eight-port OC-3, or four-port OC-12, you can repeat Steps 3 and 4 for any other ports on that card.

Step 6 Return to your originating procedure (NTP).

NTP-A206 Modify Line Settings and PM Parameter Thresholds for TXP_MR_10G Cards

Purpose	This procedure changes the line and threshold settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A249 Install the Transponder and Muxponder Cards, page 2-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the transponder card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A274 Change Card Settings for TXP_MR_10G Cards, page 13-29

- DLP-A275 Change Line Settings for TXP_MR_10G Cards, page 13-30
- DLP-A276 Change Line Threshold Settings for TXP_MR_10G Cards, page 13-32
- DLP-A277 Change Optical Thresholds Settings for TXP_MR_10G Cards, page 13-33
- DLP-A278 Change Section Trace Settings for TXP_MR_10G Cards, page 13-34
- DLP-A279 Change Optical Transport Network Settings for TXP_MR_10G Cards, page 13-35

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A274 Change Card Settings for TXP_MR_10G Cards

Purpose	This task changes the card settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_10G card where you want to change the line settings.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 Modify any of the settings described in Table 13-25.

Table 13-25 TXP_MR_10G (Transponder) Card Settings

Parameter	Description	Options
Payload Type	Sets the type of payload.	• SONET/10 GigE WAN Phy • SDH • 10 GigE LAN Phy
Termination Mode	Sets the mode of operation. For more information on Termination Mode, see the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.	• Transparent • Line

Table 13-25 TXP_MR_10G (Transponder) Card Settings (continued)

Parameter	Description	Options
Wavelength	Sets the wavelength of the DWDM side optical transmitter.	• First Tunable Wavelength • Further wavelengths in 100-GHz ITU spacing • Supported wavelengths are in white and marked by asterisks (**); non-supported wavelengths are gray
Regeneration Peer Slot	Sets the regeneration peer slot.	• None • 1 • 2 • 3 • 4 • 5 • 6 • 12 • 13 • 14 • 15 • 16 • 17

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A275 Change Line Settings for TXP_MR_10G Cards

Purpose	This task changes the line settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_10G card where you want to change the line settings.

Step 2 Click the **Provisioning > Line > SONET** tab.

Step 3 Modify any of the settings described in Table 13-26.

Table 13-26 TXP_MR_10G (Transponder) Card Line Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	• 1 • 2
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A276 Change Line Threshold Settings for TXP_MR_10G Cards

Purpose	This task changes the line threshold settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_10G card where you want to change the line threshold settings.

Step 2 Click the **Provisioning > Line Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-27.

Table 13-27 TXP_MR_10G (Transponder) Card Line Thresholds Settings

Parameter	Description	Options
Port	Port number (read-only)	• 1 • 2
CV	Coding violations	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select bullet and click **Refresh**.
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select bullet and click **Refresh**.
SEFS	Severely errored framing seconds	Numeric. Can be set for Far End, for 15-minute or one-day intervals, for Section only. Select bullet and click **Refresh**.
FC	Failure count	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A277 Change Optical Thresholds Settings for TXP_MR_10G Cards

Purpose	This task changes the optical threshold settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optical Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-28.

Table 13-28 TXP_MR_10G (Transponder) Card Optical Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	• 1 • 2
Laser Bias High (%)	Sets the warning threshold for low laser bias current.	Numeric, in percent Range 0 to 100
RX Power High (dBm)	Sets the warning threshold for high receiver input power.	Numeric, in dBm Range –40.0 to +30.0
RX Power Low (dBm)	Sets the warning threshold for low receiver input power.	Numeric, in dBm Range –40.0 to +30.0
TX Power High (dBm)	Sets the warning threshold for high transmitter output power.	Numeric, in dBm Range –40.0 to +30.0
TX Power Low (dBm)	Sets the warning threshold for low transmitter output power.	Numeric, in dBm Range –40.0 to +30.0

Step 4 Click **Apply**.

Step 5 Click the **Alarm** radio button and click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-A278 Change Section Trace Settings for TXP_MR_10G Cards

Purpose	This task changes the section trace settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_10G card where you want to change the section trace settings.

Step 2 Click the **Provisioning > Line > Section Trace** tab.

Step 3 Modify any of the settings described in Table 13-29.

Table 13-29 TXP_MR_10G (Transponder) Card Section Trace Settings

Parameter	Description	Options
Port	Sets the port number.	• 1 • 2
Trace Mode	Sets the trace mode.	• Off/None • Manual
Section Trace String Size	Sets the trace string size.	• 1 byte • 16 byte
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A279 Change Optical Transport Network Settings for TXP_MR_10G Cards

Purpose	This task changes the line optical transport network (OTN) settings for TXP_MR_10G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_10G card where you want to change the OTN settings.

Step 2 Click the **Provisioning > OTN** tabs.

Step 3 Modify any of the settings described in Tables 13-30 through 13-33.

Table 13-30 describes the values on the Provisioning > OTN > OTN Lines tab.

Table 13-30 TXP_MR_10G (Transponder) Card OTN Lines Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	2
G.709 OTN	Sets the OTN lines according to ITU-T G.709.	• Enabled • Disabled
FEC	Sets the OTN lines to forward error correction (FEC).	• Enabled • Disabled
SF BER	Sets the signal fail bit error rate.	• 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 13-31 describes the values on the Provisioning > OTN > G.709 Thresholds tab.

Table 13-31 TXP_MR_10G (Transponder) Card G.709 Threshold Settings

Parameter	Description	Options
Port	Port number (read-only)	2
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.

Table 13-31 TXP_MR_10G (Transponder) Card G.709 Threshold Settings (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select the bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select the bullet and click **Refresh**.
BBE	Background block errors	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select the bullet and click **Refresh**.
FC	Failure counter	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select the bullet and click **Refresh**.

Table 13-32 describes the values on the Provisioning > OTN > FEC Thresholds tab.

Table 13-32 TXP_MR_10G (Transponder) Card FEC Threshold Settings

Parameter	Description	Options
Port	Displays the port number (read-only)	2
Bit Errors Corrected	Sets the value of bit errors corrected.	Numeric. Can be set for 15-minute or one-day intervals.
Uncorrectable Words	Sets value of uncorrectable words.	Numeric. Can be set for 15-minute or one-day intervals.

Table 13-33 describes the values on the Provisioning > OTN > Trail Trace Identifier tab.

Table 13-33 TXP_MR_10G (Transponder) Card Trail Trace Identifier Settings

Parameter	Description	Options
Level	Sets the level.	• Section • Path
Trace Mode	Sets the trace mode.	• Off/None • Manual
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size; trail trace identifier is 64 bytes in length.
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A207 Modify Line Settings and PM Parameter Thresholds for MXP_2.5G_10G Cards

Purpose	This procedure changes the line and threshold settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A249 Install the Transponder and Muxponder Cards, page 2-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the muxponder card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A280 Change Card Settings for MXP_2.5G_10G Cards, page 13-37
- DLP-A281 Change Line Settings for MXP_2.5G_10G Cards, page 13-39
- DLP-A282 Change Line Thresholds Settings for MXP_2.5G_10G Cards, page 13-41
- DLP-A283 Change Optical Thresholds Settings for MXP_2.5G_10G Cards, page 13-42
- DLP-A284 Change Section Trace Settings for MXP_2.5G_10G Cards, page 13-43
- DLP-A285 Change Optical Transport Network Settings for MXP_2.5G_10G Cards, page 13-44

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A280 Change Card Settings for MXP_2.5G_10G Cards

Purpose	This task changes the card settings for MXP_2.5G_10G (muxponder) cards, including payload type, termination mode, and wavelength.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MXP_2.5G_10G card where you want to change the card settings.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 Modify any of the settings described in Table 13-34.

Table 13-34 MXP_2.5G_10G (Muxponder) Card Settings

Parameter	Description	Options
Payload Date Type	Sets the type of payload.	• OC3 • OC12 • OC48 • STM1 • STM4 • STM16 • 1G Ethernet • 1G Fiber Channel/FICON • 2G Fiber Channel/FICON • ESCON • DV6000 • SDI/D1 Video • HDTV • Pass Through
Termination Mode	Sets the mode of operation. For more information on Termination Mode, see the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.	• Transparent • Section • Line
Wavelength	Sets the wavelength of the DWDM side optical transmitter.	• First Tunable Wavelength • Further wavelengths in 100-GHz ITU spacing • Supported wavelengths are in white and marked by asterisks (**); non-supported wavelengths are gray

Table 13-34 MXP_2.5G_10G (Muxponder) Card Settings (continued)

Parameter	Description	Options
Regeneration Peer Slot	Sets the regeneration peer slot.	• None • 1 • 2 • 3 • 4 • 5 • 6 • 12 • 13 • 14 • 15 • 16 • 17
Regeneration Group Name	Sets the regeneration peer group name.	User defined

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A281 Change Line Settings for MXP_2.5G_10G Cards

Purpose	This task changes the line settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the MXP_2.5G_10G card where you want to change the line settings.

Step 2 Click the **Provisioning > Line > SONET** tab.

Step 3 Modify any of the settings described in Table 13-35.

Table 13-35 MXP_2.5G_10G (Muxponder) Card Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	• 1 • 2 • 3 • 4 • 5
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test
Provides Sync	If checked, the card is provisioned as a network element timing reference.	• Yes • No (Read-only)

Table 13-35 MXP_2.5G_10G (Muxponder) Card Line Settings (continued)

Parameter	Description	Options
Enable Sync Msg	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes • No
Send DoNotUse	When checked, sends a DUS (do not use) message on the S1 byte.	• Yes • No

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A282 Change Line Thresholds Settings for MXP_2.5G_10G Cards

Purpose	This task changes the line threshold settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MXP_2.5G_10G card where you want to change the line threshold settings.

Step 2 Click the **Provisioning > Line Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-36.

Table 13-36 MXP_2.5G_10G (Muxponder) Card Line Threshold Settings

Parameter	Description	Options
Port	Port number (read-only)	• 1 • 2 • 3 • 4 • 5
CV	Coding violations	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select bullet and click **Refresh**.

Table 13-36 MXP_2.5G_10G (Muxponder) Card Line Threshold Settings (continued)

Parameter	Description	Options
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select the bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select the bullet and click **Refresh**.
SEFS	Severely errored framing seconds	Numeric. Can be set for Far End, for 15-minute or one-day intervals, for Section only. Select the bullet and click **Refresh**.
FC	Failure count	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A283 Change Optical Thresholds Settings for MXP_2.5G_10G Cards

Purpose	This task changes the optical threshold settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MXP_2.5G_10G card where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-37.

Table 13-37 MXP_2.5G_10G (Muxponder) Card Optics Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	• 1 • 2 • 3 • 4 • 5
Laser Bias Low (%)	Sets the warning threshold for low laser bias current.	Numeric, in percent Range 0 to 100
RX Power High (dBm)	Sets the warning threshold for high receiver input power.	Numeric, in dBm Range –40.0 to +30.0
RX Power Low (dBm)	Sets the warning threshold for low receiver input power.	Numeric, in dBm Range –40.0 to +30.0
TX Power High (dBm)	Sets the warning threshold for high transmitter output power.	Numeric, in dBm Range –40.0 to +30.0
TX Power Low (dBm)	Sets the warning threshold for low transmitter output power.	Numeric, in dBm Range –40.0 to +30.0

Step 4 Click **Apply**.

Step 5 Click the **Alarm** radio button and click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-A284 Change Section Trace Settings for MXP_2.5G_10G Cards

Purpose	This task changes the section trace settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MXP_2.5G_10G card where you want to change the section trace settings.

Step 2 Click the **Provisioning > Line > Section Trace** tabs.

Step 3 Modify any of the settings described in Table 13-38.

Table 13-38 MXP_2.5G_10G (Muxponder) Card Section Trace Settings

Parameter	Description	Options
Port #	Sets the port number.	• 1 • 2 • 3 • 4 • 5
Trace Mode	Sets the trace mode.	• Off/None • Manual
Section Trace String Size	Sets the trace string size.	• 1 byte • 16 byte
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A285 Change Optical Transport Network Settings for MXP_2.5G_10G Cards

Purpose	This task changes the line OTN settings for MXP_2.5G_10G (muxponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the MXP_2.5G_10G card where you want to change the OTN settings.

Step 2 Click the **Provisioning > OTN** tabs.

Step 3 Modify any of the settings described in Tables 13-39 through 13-42.

Table 13-39 describes the values on the Provisioning > OTN > OTN Lines tab.

Table 13-39 MXP_2.5G_10G (Muxponder) Card OTN Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	5
G.709 OTN	Sets the OTN lines according to ITU-T G.709.	• Enabled • Disabled
FEC	Sets the OTN lines to FEC.	• Enabled • Disabled
SF BER	Sets the signal fail bit error rate.	• 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 13-40 describes the values on the Provisioning > OTN > G.709 Thresholds tab.

Table 13-40 MXP_2.5G_10G (Muxponder) Card G.709 Threshold Settings

Parameter	Description	Options
Port	Port number (read-only)	5
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
BBE	Background block errors	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
FC	Failure counter	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.

Table 13-41 describes the values on the Provisioning > OTN > FEC Thresholds tab.

Table 13-41 MXP_2.5G_10G (Muxponder) Card FEC Threshold Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	5
Bit Errors Corrected	Sets the value of bit errors corrected.	Numeric. Can be set for 15-minute or one-day intervals.
Uncorrectable Words	Sets the value of uncorrectable words.	Numeric. Can be set for 15-minute or one-day intervals.

Table 13-42 describes the values on the Provisioning > OTN > Trail Trace Identifier tab.

Table 13-42 MXP_2.5G_10G (Muxponder) Card Trail Trace Identifier Settings

Parameter	Description	Options
Level	Sets the level.	• Section • Path
Trace Mode	Sets the trace mode.	• Off/None • Manual
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size; trail trace identifier is 64 bytes in length.
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A237 Modify Line Settings and PM Parameter Thresholds for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This procedure changes the line and threshold settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A249 Install the Transponder and Muxponder Cards, page 2-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the transponder card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A471 Change Card Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-47
- DLP-A472 Change Line Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-49
- DLP-A473 Change Line Threshold Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-51
- DLP-A474 Change Optical Thresholds Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-53
- DLP-A475 Change Section Trace Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-54
- DLP-A476 Change Optical Transport Network Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards, page 13-55

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A471 Change Card Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the card settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the line settings.

Step 2 Click the **Provisioning > Card** tabs.

Step 3 Modify any of the settings described in Table 13-43.

Table 13-43 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Settings

Parameter	Description	Options
Payload Data Type	Sets the type of payload.	• OC3 • OC12 • OC48 • STM1 • STM4 • STM16 • 1G Ethernet • 1G Fiber Channel/FICON • 2G Fiber Channel/FICON • ESCON • DV6000 • SDI/D1 Video • HDTV • Pass Through **Note** If you are configuring an ISC3 connection, you must choose Pass Through.
Termination Mode	Sets the mode of operation (option only supported for SONET/SDH payloads). For more information on Termination Mode, see the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.	• Transparent • Section • Line
Wavelength	Sets the wavelength of the DWDM side optical transmitter.	• First Tunable Wavelength • Further wavelengths in 100-GHz ITU spacing • Supported wavelengths are in white and marked by asterisks (**); non-supported wavelengths are gray **Note** The four available wavelengths are listed in the Card Parameters section of the window.

Table 13-43 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Settings (continued)

Parameter	Description	Options
Regeneration Peer Slot	Sets the regeneration peer slot.	• None • 1 • 2 • 3 • 4 • 5 • 6 • 12 • 13 • 14 • 15 • 16 • 17
Regeneration Group Name	Sets the regeneration peer group name.	User defined.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A472 Change Line Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the line settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the line settings.

Step 2 Click the **Provisioning > Line > OC48** tabs.

Step 3 Modify any of the settings described in Table 13-44.

Table 13-44 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	• 1 • 2 • 3 (TXPP_MR_2.5G card only)
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate (OC-N and STM-N payloads only).	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate (OC-N and STM-N payloads only).	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Sets the automatic in-service soak period (OC-N and STM-N payloads only).	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A473 Change Line Threshold Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the line threshold settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the line threshold settings.

Step 2 Click the **Provisioning > Line Thresholds** tabs.

Step 3 Modify any of the settings as follows:

- For OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16 payloads, see Table 13-45.
- For 1G Ethernet, 1G, and 2G Fiber Channel/FICON payloads, see Table 13-46.

Table 13-45 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Line Thresholds Settings for OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16 Payloads

Parameter	Description	Options
Port	Port number (read-only)	• 1 • 2 • 3 (TXPP_MR_2.5G card only)
CV	Coding violations	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select the bullet and click **Refresh**.
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select the bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for Line (Far End only), Section, or Path. Select the bullet and click **Refresh**.
SEFS	Severely errored framing seconds (section only)	Numeric. Can be set for Far End, for 15-minute or one-day intervals for Section only. Select the bullet and click **Refresh**.

Table 13-45 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Line Thresholds Settings for OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16 Payloads (continued)

Parameter	Description	Options
FC	Failure count (line only)	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals for Line only. Select the bullet and click **Refresh**.
UAS	Unavailable seconds (line only)	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.

Table 13-46 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Line Thresholds Settings for 1G Ethernet, 1G Fiber Channel/FICON Payloads

Parameter	Description	Options
Port	Port number (read-only)	• 1 • 2 • 3 (TXPP_MR_2.5G card only)
Valid Packets	Number of valid packets	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
Invalid Packets	Number of invalid packets	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
Code Group Violations	Number of code group violations	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
Idle Ordered Sets	Number of idle ordered sets	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
Non Idle Ordered Sets	Number of non-idle ordered sets	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.
Data Code Groups	Number of data code groups (excluding ordered sets)	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, for Line only. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A474 Change Optical Thresholds Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the optical threshold settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-47.

Table 13-47 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Optics Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	• 1 • 2 • 3 (TXPP_MR_2.5G only)
Laser Bias Low (%)	Sets the warning threshold for low laser bias current.	Numeric, in percent Range 0 to 100 (client side) Range 0 to 100 (trunk side)
RX Power High (dBm)	Sets the warning threshold for high receiver input power.	Numeric, in dBm Range –40.0 to +30.0 (client side) Range –40.0 to +30.0 (trunk side)
RX Power Low (dBm)	Sets the warning threshold for low receiver input power.	Numeric, in dBm Range –40.0 to +30.0 (client side) Range –40.0 to +30.0 (trunk side)
TX Power High (dBm)	Sets the warning threshold for high transmitter output power.	Numeric, in dBm Range –40.0 to +30.0 (client side) Not applicable (trunk side)
TX Power Low (dBm)	Sets the warning threshold for low transmitter output power.	Numeric, in dBm Range –40.0 to +30.0 (client side) Not applicable (trunk side)

Step 4 Click **Apply**.

Step 5 Click the **Alarm** radio button and click **Refresh**.

Step 6 Modify any of the settings described in Table 13-28.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure (NTP).

DLP-A475 Change Section Trace Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the section trace settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the section trace settings.

Step 2 Click the **Provisioning > Line > Section Trace** tab.

Step 3 Modify any of the settings described in Table 13-48.

Table 13-48 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Section Trace Settings

Parameter	Description	Options
Port	Sets the port number.	• 1 • 2 • 3 (TXPP_MR_2.5G only)
Trace Mode	Sets the trace mode.	• Off/None • Manual
Section Trace String Size	Sets the trace string size.	• 1 byte • 16 byte
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A476 Change Optical Transport Network Settings for TXP_MR_2.5G and TXPP_MR_2.5G Cards

Purpose	This task changes the line optical transport network (OTN) settings for TXP_MR_2.5G and TXPP_MR_2.5G (transponder) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the TXP_MR_2.5G or TXPP_MR_2.5G card where you want to change the OTN settings.

Step 2 Click the **Provisioning > OTN** tabs.

Step 3 Modify any of the settings described in Tables 13-49 through 13-52.

Table 13-49 describes the values on the Provisioning > OTN > OTN Lines tab.

Table 13-49 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card OTN Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	2
G.709 OTN	Sets the OTN lines according to ITU-T G.709.	• Enabled • Disabled
FEC	Sets the OTN lines to FEC.	• Enabled • Disabled
SF BER	Sets the signal fail bit error rate.	• 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

Table 13-50 describes the values on the Provisioning > OTN > G.709 Thresholds tab.

Table 13-50 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card G.709 Threshold Settings

Parameter	Description	Options
Port[1]	Port number (read-only)	2
ES	Errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
UAS	Unavailable seconds	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
BBE	Background block errors	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.
FC	Failure counter	Numeric. Can be set for Near End or Far End, for 15-minute or one-day intervals, or for SM (OTUk) or PM (ODUk). Select bullet and click **Refresh**.

1. Latency for 1G-FC payload without G.709 is 4 microseconds, with G.709 is 40 microseconds. Latency for 2G-FC payload without G.709 is 2 microseconds, with G.709 is 20 microseconds. Consider these values when planning a FC network that is sensitive to latency.

Table 13-51 describes the values on the Provisioning > OTN > FEC Threshold tab.

Table 13-51 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card FEC Threshold Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	2
Bit Errors Corrected	Sets the value for bit errors corrected.	Numeric. Can be set for 15-minute or one-day intervals.
Uncorrectable Words	Sets the value for uncorrectable words.	Numeric. Can be set for 15-minute or one-day intervals.

Table 13-52 describes the values on the Provisioning > OTN > Trail Trace Identifier tab.

Table 13-52 TXP_MR_2.5G and TXPP_MR_2.5G (Transponder) Card Trail Trace Identifier Settings

Parameter	Description	Options
Level	Sets the level.	• Section • Path
Trace Mode	Sets the trace mode.	• Off/None • Manual
Transmit	Displays the current transmit string; sets a new transmit string.	String of trace string size; trail trace identifier is 64 bytes in length.
Expected	Displays the current expected string; sets a new expected string.	String of trace string size
Received	Displays the current received string (read only).	String of trace string size

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A90 Modify Alarm Interface Controller Settings

Purpose	This procedure provisions the AIC card to receive input from, or send output to, external devices wired to the backplane (called external alarms and controls or environmental alarms) or to change orderwire settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A32 Provision External Alarms and Controls on the Alarm Interface Controller, page 9-37 DLP-A83 Provision Orderwire, page 8-96
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the AIC card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A173 Change External Alarms Using the AIC Card, page 13-58
- DLP-A174 Change External Controls Using the AIC Card, page 13-58
- DLP-A175 Change Orderwire Settings Using the AIC Card, page 13-59

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A173 Change External Alarms Using the AIC Card

Purpose	This task changes external alarm settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 1-38 for more information.

Step 2 In node view, double-click the AIC card to display it in card view.

Step 3 Click the **Provisioning > External Alarms** tabs.

Step 4 Modify any of the following fields for each external device wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A32 Provision External Alarms and Controls on the Alarm Interface Controller" procedure on page 9-37.

- Enabled
- Alarm Type
- Severity
- Virtual Wire
- Raised When
- Description

Step 5 To provision additional devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A174 Change External Controls Using the AIC Card

Purpose	This task changes external control settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 1-38 for more information.

Step 2 In node view, double-click the AIC card to display it in card view.

Step 3 Click the **Provisioning > External Controls** tabs.

Step 4 Modify any of the following fields for each external control wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A32 Provision External Alarms and Controls on the Alarm Interface Controller" procedure on page 9-37.

- Enabled
- Trigger Type
- Control Type
- Description

Step 5 To provision additional controls, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A175 Change Orderwire Settings Using the AIC Card

Purpose	This task changes orderwire settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1 In node view, double-click the AIC card to display it in card view.

Step 2 Click the **Provisioning > Local Orderwire** tabs or **Provisioning > Express Orderwire** tabs, depending on the orderwire path that you want to create.

Step 3 If needed, adjust the Tx and Rx dBm by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. In general, you should not need to adjust the dBm.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A118 Modify Alarm Interface Controller-International Settings

Purpose	This procedure provisions the AIC-I card to receive input from or send output to external devices wired to the backplane (called external alarms and controls or environmental alarms), or to change orderwire settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International, page 9-39 DLP-A83 Provision Orderwire, page 8-96
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the AIC-I card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A208 Change External Alarms Using the AIC-I Card, page 13-60
- DLP-A209 Change External Controls Using the AIC-I Card, page 13-61
- DLP-A210 Change AIC-I Card Orderwire Settings, page 13-62

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A208 Change External Alarms Using the AIC-I Card

Purpose	This task changes external alarm settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The procedure is the same if you are using the Alarm Expansion Panel (AEP). In this case, the number of contacts that are shown on the screen is changed accordingly.

Step 1 Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 1-38 for more information.

Step 2 Double-click the AIC-I card to display it in card view.

Step 3 Click the **Provisioning > External Alarms** tabs.

Step 4 Modify any of the following fields for each external device wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International" procedure on page 9-39.

- Enabled
- Alarm Type
- Severity
- Virtual Wire
- Raised When
- Description

Step 5 To provision additional devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure (NTP).

DLP-A209 Change External Controls Using the AIC-I Card

Purpose	This task changes external control settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The procedure is the same if you are using the Alarm Expansion panel (AEP). In this case, the number of contacts that are shown on the screen is changed accordingly.

Step 1 Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task on page 1-38 for more information.

Step 2 In node view, double-click the AIC-I card to display it in card view.

Step 3 On the External Controls subtab, modify any of the following fields for each external control wired to the ONS 15454 backplane. For definitions of these fields, see the "NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International" procedure on page 9-39.

- Enabled
- Trigger Type
- Control Type

- Description

Step 4 To provision additional controls, complete Step 3 for each additional device.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-A210 Change AIC-I Card Orderwire Settings

Purpose	This task changes orderwire settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1 In node view, double-click the AIC-I card to display it in card view.

Step 2 Click the **Provisioning > Local Orderwire** tabs or the **Provisioning > Express Orderwire** tabs, depending on the orderwire path that you want to create. Provisioning steps are the same for both types of orderwire.

Step 3 If needed, adjust the Tx and Rx dBm by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. In general, you should not need to adjust the dBm.

Step 4 If you want to turn on the audible alert (buzzer) for the orderwire, check the **Buzzer On** check box.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

NTP-A91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection

Purpose	This procedure converts DS-1 and DS-3 protect cards from 1:1 to 1:N protection. This procedure does not apply to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A71 Create a 1:1 Protection Group, page 4-28
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to convert the DS-1 or DS-3 cards from 1:1 to 1:N protection. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A176 Convert DS1-14 Cards From 1:1 to 1:N Protection, page 13-63
- DLP-A177 Convert DS3-12 Cards From 1:1 to 1:N Protection, page 13-65
- DLP-A178 Convert DS3-12E Cards From 1:1 to 1:N Protection, page 13-66

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A176 Convert DS1-14 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS1-14 cards in a 1:1 protection scheme to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes DS1-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17. The DS1-14 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS1N-14 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS1N-14 card.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains Slot 3 or Slot 15 (where you will install the DS1N-14 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby (shown on page 13-64) and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they do not change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 1 through 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS1-14 cards that you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection group does not disrupt service. However, no protection bandwidth exists for the working circuits until you complete the 1:N protection procedure. Therefore, complete this procedure as quickly as possible.

Step 10 If needed, repeat Steps 7 to 9 for other DS-1 1:1 protection groups that you want to include in a 1:N group.

Step 11 Physically remove the DS1-14 card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 12 In node view, right-click the slot that held the removed card and select **Delete** from the drop-down menu. Wait for the card to disappear from node view.

Step 13 Physically insert a DS1N-14 card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS1N-14.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 From the Type drop-down menu, choose **1:N (card)**.

Step 20 From the Protect Card drop-down menu, choose the DS1N-14 card. Verify that the correct DS1N-14 card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 22 If necessary, set a new reversion time in the Reversion time drop-down menu.

Note 1:N protection groups are always revertive.

Step 23 Click **OK**. The protection group appears in the Protection Groups list on the Protection subtab.

Step 24 Return to your originating procedure (NTP).

DLP-A177 Convert DS3-12 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3-12 cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes that DS3-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17. The DS3-12 cards in Slots 3 or 15, which are the protection slots, will be replaced with DS3N-12 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS3N-12 card and a protection group with DS3-12 cards.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group containing Slot 3 or Slot 15 (where you will install the DS3N-12 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby as shown on page 13-64, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Therefore, complete this procedure as soon as possible.

Step 10 If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.

Step 11 Physically remove the protect DS3-12 card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 12 In node view, right-click the slot that held the removed card and choose **Delete** from the drop-down menu. Wait for the card to disappear from the node view.

Step 13 Physically insert a DS3N-12 card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS3N-12 card.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 Click **Type** and choose **1:N (card)** from the drop-down menu.

Step 20 Verify that the DS3N-12 card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 22 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 23 Return to your originating procedure (NTP).

DLP-A178 Convert DS3-12E Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3-12E cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This task assumes that DS3-12E cards are installed in Slots 1 to 6 and/or Slots 12 to 17. The DS3-12E cards in Slots 3 or 15, which are the protection slots, will be replaced with DS3N-12E cards. The procedure requires at least one DS3N-12E card and a protection group with DS3-12E cards.

Step 1 In node view, click the **Maintenance > Protection** tab.

Step 2 Click the protection group containing Slot 3 or Slot 15 (where you will install the DS3N-12E card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby as shown on page 13-64, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12E cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tab.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Do not delay when completing this procedure.

Step 10 If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.

Step 11 Physically remove the protect DS3-12E card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 12 In node view, right-click the slot that held the removed card and choose **Delete** from the drop-down menu. Wait for the card to disappear from the node view.

Step 13 Physically insert a DS3N-12E card into the same slot.

Step 14 Verify that the card boots up properly.

Step 15 Click the **Inventory** tab and verify that the new card appears as a DS3N-12E.

Step 16 Click the **Provisioning > Protection** tabs.

Step 17 Click **Create**.

Step 18 Type a name for the protection group in the Name field (optional).

Step 19 Click **Type** and choose **1:N (card)** from the drop-down menu.

Step 20 Verify that the DS3N-12E card appears in the Protect Card field.

Step 21 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 22 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 23 Return to your originating procedure (NTP).

NTP-A229 Modify Line Settings and PM Parameter Thresholds for Optical Service Channel Cards

Purpose	This procedure changes the line and threshold settings for optical service channel cards (OSCM and OSC-CSM). This procedure applies to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A242 Install the DWDM Cards, page 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the OSCM or OSC-CSM card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A477 Change Optical Line Settings for OSCM and OSC-CSM Cards, page 13-68
- DLP-A478 Change Line Threshold Settings for OSCM and OSC-CSM Cards, page 13-70
- DLP-A479 Change Optical Line Parameters for OSCM and OSC-CSM Cards, page 13-71
- DLP-A480 Change Channel Settings for OSCM and OSC-CSM Cards, page 13-72
- DLP-A525 Change Maintenance Settings for Automatic Laser Shutdown, page 13-73

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A477 Change Optical Line Settings for OSCM and OSC-CSM Cards

Purpose	This task changes the line settings for OSCM and OSC-CSM cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OSCM or OSC-CSM card where you want to change the line settings.

Step 2 Click the **Provisioning > OC3 Line > OC3 Line** tabs.

Step 3 Modify any of the settings described in Table 13-53.

Table 13-53 OSCM and OSC-CSM Card OC-3 Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	—
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference.	• Checked • Unchecked (Read-only)
Enable Synch Messages	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Checked • Unchecked
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte.	• Checked • Unchecked
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port.	• On • Off (Read-only)
State	Places port in or out of service.	• In Service • Out of Service • Out of Service MT • Out of Service AINS
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
Type	Defines the port as SONET or SDH. The Enable Sync Msg field and the Send Do Not Use field must be disabled before the port can be set to SDH.	• Sonet • SDH

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A478 Change Line Threshold Settings for OSCM and OSC-CSM Cards

Purpose	This task changes the optical line threshold settings for OSCM and OSC-CSM cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OSCM or OSC-CSM card where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > OC3 Line > SONET Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-54.

Table 13-54 OSCM and OSC-CSM Cards Optical Threshold Settings

Parameter	Description	Options
Port	Port number	—
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals for Line or Section (Near and Far End). Select the bullet and click **Refresh**.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Section (Near and Far End). Select the bullet and click **Refresh**.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Section (Near and Far End). Select the bullet and click **Refresh**.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals for Line or Section. Select the bullet and click **Refresh** or Path (Near and Far End)
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Section (Near and Far End). Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A479 Change Optical Line Parameters for OSCM and OSC-CSM Cards

Purpose	This task changes the optical line settings for OSCM and OSC-CSM cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OSCM or OSC-CSM card where you want to change the line settings.

Step 2 Click the **Provisioning > Optical Line > Parameters** tabs.

Step 3 Modify any of the settings described in Table 13-55.

Table 13-55 OSCM and OSC-CSM Card Line Settings

Parameter	Description	Options
Port #	Displays the port number and TX or RX.	Read-only
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
Status	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
Line Direction	Provides the ability to associate a card with the line direction. Use this field if you have two cards and must designate which one will carry the traffic flow from east to west. The second card will carry traffic from west to east.	• East to West • West to East
Type	Identifies the type of port, such as Input Com, Output Com, Input Line, Output Line, Input OSC, and Output OSC.	Read only
Power	Shows the current power level per port.	Read only

Table 13-55 OSCM and OSC-CSM Card Line Settings (continued)

Parameter	Description	Options
VOA Mode	Shows the current functional mode of the variable optical attenuator (VOA): constant gain mode, constant power mode, or not in use (N/A).	Read only
VOA Power Ref.	Shows the value of the optical output power going to a VOA when constant power mode is active. Automatic node setup (ANS) is the only function that can modify this value.	Read only
VOA Power Calib.	The user can modify the optical output power to the VOA if necessary. This feature is normally used when the system is configured as "access" in Provisioning > WDM-ANS.	Numeric
VOA Attenuation Ref.	Shows the attenuation value of the VOA when the VOA is set in constant attenuation mode. ANS and amplifier power control (APC) are the only functions that can modify this value.	Read only
VOA Attenuation Calib.	The user can modify the attenuation value of the VOA if necessary when the VOA mode is set for constant attenuation.	Numeric

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A480 Change Channel Settings for OSCM and OSC-CSM Cards

Purpose	This task changes the optical channel threshold settings for OSCM and OSC-CSM cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OSCM or OSC-CSM card where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optical Line > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-56.

Table 13-56 OSCM and OSC-CSM Cards Optical Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	—
Power Low (dBm)	Set the low power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.
Power High (dBm)	Set the high power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A525 Change Maintenance Settings for Automatic Laser Shutdown

Purpose	This task changes the maintenance settings the automatic laser shutdown (ALS) feature on the OSC-CSM, OSCM, and OPT-BST amplifier cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OSC-CSM, OSCM, or OPT-BST amplifier where you want to change the line settings.

Step 2 Click the **Maintenance > ALS** tabs.

Step 3 Modify any of the settings described in Table 13-57.

Table 13-57 OSC-CSM, OSCM, or OPT-BST Amplifier Maintenance Settings

Parameter	Description	Options
OSRI	Optical safety remote interlock. Shuts down the optical output power. When set to "On" the amplifier cannot be unknowingly turned on.	On and off
ALS Mode	Automatic laser shutdown. Provides the ability to automatically shut a potentially hazardous laser off.	• Disable • Auto Restart • Manual Restart • Manual Restart for Test

Table 13-57 OSC-CSM, OSCM, or OPT-BST Amplifier Maintenance Settings (continued)

Parameter	Description	Options
Recovery Pulse Duration	Displays the duration of the optical power pulse that begins when an amplifier restarts.	Read only
Recovery Pulse Interval	Displays the interval between optical power pulses.	Read only
Currently Shutdown	Displays the current status of the laser	Read only
Request Laser Restart	If checked, allows you to restart the laser.	Checked or unchecked

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A230 Modify Line Settings and PM Parameter Thresholds for Amplifier Cards

Purpose	This procedure changes the line and threshold settings for the OPT-PRE and OPT-BST amplifier cards. This procedure applies to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A242 Install the DWDM Cards, page 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the OPT-PRE or OPT-BST amplifier card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A525 Change Maintenance Settings for Automatic Laser Shutdown, page 13-73
- DLP-A481 Change Optical Line Settings for OPT-PRE and OPT-BST Amplifiers, page 13-75
- DLP-A482 Change Line Threshold Settings for OPT-PRE and OPT-BST Amplifiers, page 13-76
- DLP-A483 Change Optical Amplifier Line Settings for OPT-PRE and OPT-BST Amplifiers, page 13-77
- DLP-A484 Change Channel Settings for OPT-PRE and OPT-BST Amplifiers, page 13-78

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A481 Change Optical Line Settings for OPT-PRE and OPT-BST Amplifiers

Purpose	This task changes the line settings for OPT-PRE and OPT-BST amplifier cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OPT-PRE or OPT-BST amplifier where you want to change the line settings.

Step 2 Click the **Provisioning > Optical Line > Parameters** tabs.

Step 3 Modify any of the settings described in Table 13-58.

Table 13-58 OPT-PRE and OPT-BST Amplifier Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	Displays port number and TX or RX.
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
Status	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
Line Direction	Provides the ability to associate a card with the line direction. Use this field if you have two cards in the same shelf and must designate which one will carry the traffic flow from east to west. The second card will carry traffic from west to east.	• East to West • West to East
Type	Identifies the type of port, such as Input Com, Output Com, Input Line, Output Line, Input OSC, and Output OSC.	Read only
Power	Shows the current power level per port.	Read only

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A482 Change Line Threshold Settings for OPT-PRE and OPT-BST Amplifiers

Purpose	This task changes the optical line threshold settings for OPT-PRE and OPT-BST amplifier cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OPT-PRE or OPT-BST amplifier where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optical Line > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-59.

Table 13-59 OPT-PRE and OPT-BST Amplifiers Optical Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	—
Power Low (dBm)	Set the low power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.
Power High (dBm)	Set the high power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A483 Change Optical Amplifier Line Settings for OPT-PRE and OPT-BST Amplifiers

Purpose	This task changes the optical amplifier line settings for OPT-PRE and OPT-BST amplifier cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OPT-PRE or OPT-BST amplifier where you want to change the line settings.

Step 2 Click the **Provisioning > Opt. Ampli. Line > Parameters** tabs.

Step 3 Modify any of the settings described in Table 13-60.

Table 13-60 OSCM and OSC-CSM Card Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	Displays port number and TX or RX.
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
Status	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
Line Direction	Provides the ability to associate a card with the line direction. Use this field if you have two cards in the same shelf and must designate which one will carry the traffic flow from east to west. The second card will carry traffic from west to east.	• East to West • West to East
Type	Identifies the type of port, such as Input Com, Output Com, Input Line, Output Line, Input OSC, and Output OSC.	Read only
Power	Shows the current power level per port.	Read only
Power Ref.	Shows the optical power per channel leaving to the amplifier.	Read only
Power Calib.	The user can manually set the total optical power going to the amplifiers.	Numeric

Table 13-60 OSCM and OSC-CSM Card Line Settings (continued)

Parameter	Description	Options
Gain	The current gain of the amplifiers.	Read only
Gain Set Point	The value of the gain that the amplifier must achieve.	Read only or numeric depending on mode setting. When the system is configured as metro core, this field is read only. When the system is configured as metro access this field can be changed by the user.
Tilt Reference	This field is set to zero. It represents the default value for the amplifier tilt. In a future software release this value will be managed by APC.	Read only
Tilt Calibration	The user can manually set the amplifier tilt.	Numeric
Mode	Shows the working mode of the amplifier: control gain or control power.	Read only

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A484 Change Channel Settings for OPT-PRE and OPT-BST Amplifiers

Purpose	This task changes the optical channel threshold settings for OPT-PRE and OPT-BST amplifier cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OPT-PRE or OPT-BST amplifier where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-61.

Table 13-61 OPT-PRE and OPT-BST Cards Optical Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	—

Table 13-61 OPT-PRE and OPT-BST Cards Optical Thresholds Settings (continued)

Parameter	Description	Options
Power Low (dBm)	Set the low power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.
Power High (dBm)	Set the high power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A231 Modify Line Settings and PM Parameter Thresholds for Multiplexer and Demultiplexer Cards

Purpose	This procedure changes the line and threshold settings for the multiplexer and demultiplexer. The cards included in this category are the 32 MUX, 32 DMX, and the 4MD xx.x cards. This procedure applies to DWDM-only nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-A242 Install the DWDM Cards, page 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Refer to the *Cisco ONS 15454 Reference Manual* for more information on MUX and DMX parameters.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the 32 MUX, 32 DMX, or 4MD xx.x card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A485 Change Optical Line Settings for Multiplexer and Demultiplexer Cards, page 13-80
- DLP-A486 Change Line Threshold Settings for Multiplexer and Demultiplexer Cards, page 13-81
- DLP-A487 Change Optical Channel Settings for Multiplexer and Demultiplexer Cards, page 13-81
- DLP-A488 Change Channel Settings for Multiplexer and Demultiplexer Cards, page 13-84

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A485 Change Optical Line Settings for Multiplexer and Demultiplexer Cards

Purpose	This task changes the optical line settings for 32 MUX, 32 DMX, and 4MD xx.x multiplexer and demultiplexer cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the multiplexer or demultiplexer cards where you want to change the line settings.

Step 2 Click the **Provisioning > Optical Line > Parameters** tabs.

Step 3 Modify any of the settings described in Table 13-62.

Table 13-62 Multiplexer and Demultiplexer Card Optical Line Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	Displays port number and TX or RX.
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
Status	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
Line Direction	Provides the ability to associate a card with the line direction. Use this field if you have two cards and must designate which one will carry the traffic flow from east to west. The second card will carry traffic from west to east.	• East to West • West to East
Type	Identifies the type of port, such as Input Com, Output Com, Input Line, Output Line, Input OSC, and Output OSC.	Read only
Power	Shows the current power level per port.	Read only

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A486 Change Line Threshold Settings for Multiplexer and Demultiplexer Cards

Purpose	This task changes the optical line threshold settings for 32 MUX, 32 DMX, and 4MD xx.x multiplexer and demultiplexer cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the multiplexer or demultiplexer cards where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optical Line > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-63.

Table 13-63 Multiplexer and Demultiplexer Card Line Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	—
Power Low (dBm)	Set the low power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.
Power High (dBm)	Set the high power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A487 Change Optical Channel Settings for Multiplexer and Demultiplexer Cards

Purpose	This task changes the optical channel settings for 32 MUX, 32 DMX, and 4MD xx.x multiplexer and demultiplexer cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the multiplexer or demultiplexer card where you want to change the line settings.

Step 2 Click the **Provisioning > Optical Chn > Parameters** tabs.

Step 3 Modify any of the settings described in Table 13-64.

Table 13-64 Multiplexer and Demultiplexer Card Optical Channel Settings

Parameter	Description	Options
Port #	Displays the port number (read-only).	Displays port number and TX or RX.
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
Status	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
Line Direction	Provides the ability to associate a card with the line direction. Use this field if you have two cards in the same shelf and must designate which one will carry the traffic flow from east to west. The second card will carry traffic from west to east.	• East to West • West to East
Type	Identifies the type of port, such as Input Com, Output Com, Input Line, Output Line, Input OSC, and Output OSC.	Read only
Power	Shows the current power level per port.	Read only
VOA Mode	Shows the current functional mode of the VOA: constant power or constant attenuation.	Read only
VOA Power Ref.	Shows the value of the optical output power going to a VOA when constant power mode is active. Dmux shows the reference value of the desired optical power going to the client. ANS is the only function that can modify this value (using the Pdrop parameter on the Provisioning tab). Mux show the reference value of the desired per channel optical power. ANS is the only function that can modify this value (using the Port Mux Stage parameter on the Provisioning tab).	Read only

Table 13-64 Multiplexer and Demultiplexer Card Optical Channel Settings (continued)

Parameter	Description	Options
VOA Power Calib.	The user can modify the optical output power to the VOA if necessary. The VOA power calibration offsets the VOA power reference. Dmux allows you to modify the optical output power to the client if necessary. Mux allows you to modify the output power per channel. This feature is normally used when the system is configured as “access” in Provisioning > WDM-ANS.	Numeric
VOA Attenuation Ref.	Shows the attenuation value of the VOA when the VOA is set in attenuation mode. ANS and APC are the only functions that can modify this value.	Read only
VOA Attenuation Calib.	Allows the user to modify the attenuation value of the VOA if necessary when the VOA mode is set for constant attenuation.	Numeric
Actual Wavelength	Shows the wavelength specified by the manufacturing data. This field cannot be set manually.	Read only
Expected Wavelength	Shows the preprovisioned wavelength. This field is used to preprovsion cards. For example, you can specify a generic AD-1C in Slot 15 and set the expected wavelength to 1552.52. The result is a AD-1C-52.5. If the actual equipment installed does not match the preprovisioned slot, an MEA Mismatch Equipment Alarm occurs.	Numeric

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A488 Change Channel Settings for Multiplexer and Demultiplexer Cards

Purpose	This task changes the optical channel threshold settings for 32 MUX, 32 DMX, and 4MD xx.x multiplexer and demultiplexer cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the multiplexer or demultiplexer cards where you want to change the optical threshold settings.

Step 2 Click the **Provisioning > Optical Chn > Optics Thresholds** tabs.

Step 3 Modify any of the settings described in Table 13-65.

Table 13-65 Multiplexer and Demultiplexer Cards Optical Thresholds Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	—
Power Low (dBm)	Set the low power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.
Power High (dBm)	Set the high power settings.	Numeric. Can be set for 15-minute or one-day intervals for Warning or Alarm. Select the bullet and click **Refresh**.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-A259 Modify Line Settings and PM Parameter Thresholds for FC_MR-4 Cards

Purpose	This procedure changes the line and threshold settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A274 Install the FC_MR-4 Cards, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to change the OC-N card settings. If you are already logged in, proceed to Step 2.

Step 2 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Perform any of the following tasks as needed:

- DLP-A419 Change Port Settings for the FC_MR-4 Card, page 13-85
- DLP-A420 Create Threshold Settings for FC_MR-4 Cards, page 13-86
- DLP-A432 Delete Threshold Settings for FC_MR-4 Cards, page 13-88

Step 4 Complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Stop. You have completed this procedure.

DLP-A419 Change Port Settings for the FC_MR-4 Card

Purpose	This task changes the port settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning > Port** tabs.

Step 3 Modify any of the settings described in Table 13-66.

Table 13-66 FC_MR-4 Card Port Settings

Parameter	Description	Options
#	Displays the port number (read-only).	1 through 4
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 8-11.
State	Places port in service, out of service, or out of service-maintenance.	• IS • OOS • OOS_MT
Port Rate	Selects the fiber channel interface.	• 1 Gbps • 2 Gbps
Link Rate	Displays the actual rate of the port.	—

Table 13-66 FC_MR-4 Card Port Settings (continued)

Parameter	Description	Options
Max GBIC Rate	Displays the maximum Gigabit Interface Converter (GBIC) rate. Cisco supports two GBICs for the FC_MR-4 card (ONS-GX-2FC-SML and ONS-GX-2FC-MMI). If used with another GBIC, "Contact GBIC vendor" displays.	—
Enable Link Recovery	Enables or disables link recovery if a local port is inoperable. If enabled, a link reset occurs when there is a loss of transport from a cross-connect switch, a protection switch, or an upgrade.	—

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A420 Create Threshold Settings for FC_MR-4 Cards

Purpose	This task creates threshold settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to change the threshold settings.

Step 2 Click the **Provisioning > Line Thresholds** tabs.

Step 3 Click **Create**.

Step 4 In the Create Fmcr Threshold dialog box, complete the following:

- Slot—(Display only) Displays the selected FC_MR-4 slot.
- Port—Choose the FC_MR-4 port from the drop-down menu (1 through 4 or All).
- Variable—Choose a variable described in Table 13-67.

Table 13-67 FC_MR-4 Variables

Variable	Description
fibreStats8B10BErrors	Receive invalid ordered sets (8B/10B encoding) error counter
fibreStatsEncodingDispErrors	Receive disparity violation counter
fibreStatsRxUndersizedFrames	Receive undersize frame counter

Table 13-67 FC_MR-4 Variables (continued)

Variable	Description
fibreStatsRxOversizedFrames	Receive oversize frame counter
fibreStatsRxFramesBadCRC	Receive frame cyclic redundancy check (CRC) error counter
fibreStatsRxFrames	Receive frame counter
fibreStatsRxBytes	Receive frame octets counter
fibreStatsTxFramesBadCRC	Transmit frame CRC error counter
fibreStatsTxFrames	Transmit frame counter
fibreStatsTxBytes	Transmit frame octets counter
fibreStatsLinkResets	Link resets detected by the link recovery feature
gfpStatsRxSBitErrors	Receive single bit errored core header count
gfpStatsRxMBitErrors	Receive multibit errored core header count
gfpStatsRxTypeInvalid	Receive invalid generic framing procedure (GFP) type error count
gfpStatsRxSblkCRCErrors	Receive super-block CRC error count

- Alarm Type—Choose the alarm type:
  - Rising—Indicates that the current sampled value is greater than or equal to the Rising Threshold.
  - Falling—Indicates that the current sampled value is less than or equal to the Falling Threshold.
  - Rising and Falling—Indicates that the current sampled value crosses either threshold.
- Sample Type—Choose one of the following:
  - Relative—Tests the difference between the current value and the value in the last interval.
  - Absolute—Tests only the current value.
- Sample Period—Type the number of seconds in a sample period (a minimum of 10 seconds).
- Rising Threshold—Type the upper threshold value for the sampled variable (1 through 2147483647).
- Falling Threshold—Type the lower threshold value for the sampled variable (1 through 2147483647). This value must be less than or equal to the Rising Threshold.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-A432 Delete Threshold Settings for FC_MR-4 Cards

Purpose	This task deletes a threshold setting for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to delete a threshold setting.

Step 2 Click the **Provisioning > Line Thresholds** tabs.

Step 3 Click the threshold setting that you want to remove. To select multiple threshold settings, press **Ctrl** and click.

Step 4 Click **Delete**.

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

CHAPTER 14

Upgrade Cards and Spans

This chapter explains how to upgrade common control cards, DS3-12 and DS3N-12 cards, and optical spans for the Cisco ONS 15454.

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.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A92 Upgrade the XC Card to the XCVT Card, page 14-2—Complete as needed.
2. NTP-A220 Upgrade the XC or XCVT Card to the XC10G Card, page 14-3—Complete as needed
3. NTP-A93 Upgrade the DS3-12 Card to the DS3-12E Card, page 14-4—Complete as needed.
4. NTP-A153 Upgrade the AIC Card to AIC-I, page 14-8—Complete as needed.
5. NTP-A94 Upgrade OC-N Cards and Spans Automatically, page 14-8—Complete this procedure as needed to upgrade OC-N cards within path protection configurations, BLSRs, and 1+1 protection groups.
6. NTP-A95 Upgrade OC-N Spans Manually, page 14-11—Complete this procedure as needed to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).

NTP-A92 Upgrade the XC Card to the XCVT Card

Purpose	This procedure upgrades the XC card to the XCVT card.
Tools/Equipment	Two XCVT cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note The UNEQ-P alarm is raised during a cross-connect card upgrade if you have E100T-12/E1000-2 cards installed in the node. The alarm will clear within a few seconds.

Caution Always upgrade the standby cross-connect card. Removing an active cross-connect card can cause a protection switch unless a lockout is in place. If the standby card is being upgraded, a lockout is unnecessary.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Determine the standby XC card. The ACT/STBY LED of the standby XC card is amber, while the ACT/STBY LED of the active XC card is green.

Step 4 Physically replace the standby XC card with an XCVT card:

a. Open the XC card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

c. Open the ejectors on the XCVT card.

d. Slide the XCVT card into the slot along the guide rails.

e. Close the ejectors.

On the XCVT card the FAIL LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The amber ACT/STBY LED turns on.

Step 5 In node view, click the **Maintenance > Cross-Connect** tabs.

Step 6 From the Cross Connect Cards menu, choose **Switch**.

Step 7 Click **Yes** on the Confirm Switch dialog box. Traffic switches to the XCVT card inserted in Step 4. The ACT/STBY LED on this card changes from amber to green.

Note The Interconnection Equipment Failure alarm appears, but it will clear when the upgrade procedure is complete and the node has matching cross-connect cards installed.

Step 8 Physically remove the now standby XC card from the shelf and insert the second XCVT card into the empty XC slot:

a. Open the XC card ejectors.

b. Slide the XC card out of the slot.

c. Open the ejectors on the XCVT.

d. Slide the XCVT card into the slot along the guide rails.

e. Close the ejectors.

The upgrade is complete when the second XCVT card boots up and becomes the standby XCVT.

Stop. You have completed this procedure.

NTP-A220 Upgrade the XC or XCVT Card to the XC10G Card

Purpose	This procedure upgrades an XC or XCVT card to an XC10G card.
Tools/Equipment	Two XC10G cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note This procedure only applies to the XC or XCVT cards that are installed in the 15454-SA-ANSI or the 15454-SA-HD. You cannot perform this upgrade from shelves released prior to Software R3.1. The XC10G requires the 15454-SA-ANSI or the 15454-SA-HD.

Note The UNEQ-P alarm is raised during a cross-connect card upgrade if you have E100T-12/E1000-2 cards installed in the node. The alarm will clear within a few seconds.

Note Downgrade procedures from XC10G cards to XCVT or XC cards are not supported. Contact Cisco Technical Assistance Center (TAC) for more information see the "Obtaining Technical Assistance" section on page lviii.

Caution Always upgrade the standby cross-connect card. Removing an active cross-connect card can cause a protection switch unless a lockout is in place. If the standby card is being upgraded, a lockout is unnecessary.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Determine the standby XC or XCVT card. The ACT/STBY LED of the standby XC or XCVT card is amber, while the ACT/STBY LED of the active XC or XCVT card is green.

Step 4 Physically replace the standby XC or XCVT card on the ONS 15454 with an XC10G card:

a. Open the XC or XCVT card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

c. Open the ejectors on the XC10G card.

d. Slide the XC10G card into the slot along the guide rails.

e. Close the ejectors.

Note On the XC10G card the fail LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The ACT/STBY LED turns amber and remains on. In node view, the XC10G appears as the standby XC or XCVT.

Step 5 In node view, click the **Maintenance > Cross-Connect** tabs.

Step 6 From the Cross Connect Cards menu, choose **Switch**.

Step 7 Click **Yes** on the Confirm Switch dialog box. Traffic switches to the XC10G card you inserted in Step 4. The ACT/STBY LED on this card changes from amber to green.

Note The Interconnection Equipment Failure alarm appears, but it will clear when the upgrade procedure is complete and the node has matching cross-connect cards installed.

Step 8 Physically remove the now standby XC or XCVT card from the ONS 15454 and insert the second XC10G card into the empty XC or XCVT card slot:

a. Open the XC or XCVT card ejectors.

b. Slide the XC or XCVT card out of the slot.

c. Open the ejectors on the XC10G card.

d. Slide the XC10G card into the slot along the guide rails.

e. Close the ejectors.

The upgrade is complete when the second XC10G card boots up and becomes the standby XC10G card. In node view, both the active and standby cards will change to XC10G.

Stop. You have completed this procedure.

NTP-A93 Upgrade the DS3-12 Card to the DS3-12E Card

Purpose	This procedure upgrades the DS3-12 card to the DS3-12E card or the DS3N-12 card to the DS3N-12E card. This procedure can also be used to enable the capabilities of a DS3-12E card that was installed in a shelf with Software R3.1 or earlier.
Tools/Equipment	DS3-12E or DS3N-12E card

Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Upgrades must be performed between two N-type cards or two non-N-type cards. You cannot upgrade between an N-type card and a non-N-type card. When physically replacing a card, the new card must be in the same slot as the old card. The DS3-12E card upgrade supports 1:1 and 1:N protection schemes. The procedure is non-service affecting for protected cards; that is, the upgrade will cause a switch less than 50 ms in duration.

Caution Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.

Note During the upgrade some minor alarms and conditions appear and then clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms if you are upgrading protected cards. (Upgrading an unprotected card can be service affecting.) If any service-affecting alarms occur, Cisco recommends backing out of the procedure. See the "NTP-A254 Downgrade a DS3-12E/DS3NE Card to a DS3-12/DS3N-12 Card" procedure on page 14-6.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Determine if the card you are upgrading is protected or unprotected:

a. A protected card will be listed under Protection Groups in the **Maintenance > Protection** tabs. The slot, port, and status (that is, Protect/Standby, Working/Active) of each card will be listed in the Selected Group.

b. An unprotected card will not be listed in the Protection Groups/Selected Group in the **Maintenance > Protection** tabs.

Caution Traffic will be lost during an upgrade on an unprotected card.

Step 4 If the card you are upgrading is unprotected, skip this step and go to Step 5 and ignore references to the protect card and protect slot. If the card you are upgrading is protected, make sure the protect card is not active. If the card status is Protect/Active, perform a switch so that the working card becomes active:

a. Double-click the protection group.

b. Click the Protect/Active card.

c. Click **Switch.**

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

Step 5 Physically remove the protect DS3-12 or the protect DS3N-12 card:

a. Open the DS3-12 or DS3N-12 card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 6 Right-click the protect slot and choose **Change Card** from the drop-down menu.

Step 7 Choose the new card (DS3-12E or DS3N-12E) from the Change to: drop-down menu.

Step 8 Click **OK**.

Step 9 Insert the new DS3-12E or DS3N-12E card into the protect slot:

a. Open the ejectors on the DS3-12E or DS3N-12E card.

b. Slide the DS3-12E or DS3N-12E card into the slot along the guide rails.

Step 10 Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby.

Step 11 If you switched traffic in Step 4, clear the switch:

a. In the **Maintenance** > **Protection** tabs, double-click the protection group that contains the reporting card.

b. Click the selected group.

c. Click **Clear** and click **Yes** at the confirmation dialog box.

Step 12 Repeat Steps 3 through 11 for the working card.

Stop. You have completed this procedure.

NTP-A254 Downgrade a DS3-12E/DS3NE Card to a DS3-12/DS3N-12 Card

Purpose	This task downgrades a DS3-12E or DS3NE card. Downgrading can be performed to back out of an upgrade.The procedure for downgrading is the same as upgrading except you choose DS3-12 or DS3N-12 from the Change Card drop-down menu.
Tools	None
Prerequisite Procedures	NTP-A17 Install the Electrical Cards, page 2-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note All ports must be provisioned as UNFRAMED and have Path Trace disabled.

Note Working cards must be downgraded before protect cards.

Tip The procedure for downgrading is the same as upgrading except you choose DS3-12 or DS3N-12 from the Change Card drop-down menu.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Determine if the card you are downgrading is protected or unprotected:

a. A protected card will be listed in the Protection Groups area on the **Maintenance > Protection** tabs. The slot, port, and status (that is, Protect/Standby, Working/Active) of each card will be listed under Selected Group.

b. An unprotected card will not be listed under Protection Groups/Selected Group in the **Maintenance > Protection** tabs.

Caution Traffic will be lost during an upgrade on an unprotected card.

Step 4 If the card you are upgrading is unprotected, skip this step and go to Step 5 and ignore references to the protect card and protect slot. If the card you are upgrading is protected, make sure the protect card is not active. If the card status is Protect/Active, perform a switch so that the working card becomes active:

a. Double-click the protection group.

b. Click the Protect/Active card.

c. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 5 Physically remove the working DS3-12E card or the working DS3N-12E card:

a. Open the DS3-12E or DS3N-12E card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the downgrade is complete.

Step 6 Right-click the slot to be downgraded and choose **Change Card** from the drop-down menu.

Step 7 Choose **DS3-12** or **DS3N-12** from the Change to: drop-down menu.

Step 8 Click **OK**.

Step 9 Insert the DS3-12 or DS3N-12 card into the working slot:

a. Open the ejectors on the DS3-12 or DS3N-12 card.

b. Slide the DS3-12 or DS3N-12 card into the slot along the guide rails.

Step 10 Close the ejectors. Wait for the IMPROPRMVL alarm to clear and the card to become active.

Step 11 If you switched traffic in Step 4, clear the switch:

a. In the **Maintenance** > **Protection** tabs, double-click the protection group that contains the reporting card.

b. Click the selected group.

c. Click **Clear** and click **Yes** in the confirmation dialog box.

Step 12 Repeat Steps 3 through 11 to downgrade the protect card if applicable.

Stop. You have completed this procedure.

NTP-A153 Upgrade the AIC Card to AIC-I

Purpose	This procedure upgrades an AIC card to an AIC-I card; the AIC-I card provides additional alarm contacts.
Tools	None
Prerequisite Procedures	DLP-A38 Install the Alarm Interface Controller or Alarm Interface Controller–International Card, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Step 1 Physically remove the AIC card:

a. Open the AIC card ejectors.

b. Slide the card out of the slot.

After several seconds this raises the IMPROPRMVL alarm, which will clear when the downgrade is complete.

Step 2 Complete the "DLP-A38 Install the Alarm Interface Controller or Alarm Interface Controller–International Card" task on page 2-11.

Step 3 Complete the "NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International" procedure on page 9-39.

Stop. You have completed this procedure.

NTP-A94 Upgrade OC-N Cards and Spans Automatically

Purpose	This procedure upgrades cards, two-fiber BLSR spans, four-fiber BLSR spans, path protection spans, and 1+1 protection group spans. The Span Upgrade Wizard only supports OC-N span upgrades. It does not support electrical upgrades.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade (for example, XC10G cards and OC-48 any slot cards) Attenuators might be needed for some applications
Prerequisite Procedures	The span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Do not perform any other maintenance operations, such as facility or terminal loopbacks, or add any circuits during a card or span upgrade.

Note OC-N transmit and receive levels should be in their acceptable range as shown in the specifications for each card in the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Note During the upgrade, the IMPROPRMVL alarm may be raised. It will clear automatically.

Note A four-port OC-3 to eight-port OC-3 upgrade, or an OC-12 to four-port OC-12 upgrade can only be performed from multispeed slots (Slots 1 to 4 and 14 to 17) because the OC3-8 and OC12-4 card can only be installed in multispeed slots. Ensure that the OC-3 and OC-12 cards are in multispeed slots before performing a span upgrade to the OC3-8 and OC12-4. The four OC-3 ports will be mapped to Ports 1 to 4 on the eight-port OC-3 card. The OC-12 port will be mapped to Port 1 on the four-port OC-12 card.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48) which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19. To create circuits, see Chapter 8, "Create Circuits and VT Tunnels."

Step 1 Determine the type of upgrade you need to make and be sure you have the necessary cards.Valid card upgrades include:

- Four-port OC-3 to eight-port OC-3
- Single-port OC-12 to four-port OC-12

Valid span upgrades include:

- Single-port OC-12 to OC-48
- Single-port OC-12 to OC-192
- OC-48 to OC-192

Caution You cannot upgrade a four-port OC-12 span. If the ring contains any OC12-4 cards and you need to upgrade all the spans in the ring, you will need to downgrade the OC12-4 card to a single-port OC-12 card (which is only possible if one port on the OC12-4 card is being used).

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 3.

> **Note** The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present; for example, no upgrade is possible from an OC-48 span unless XC10G cards are installed in the nodes at both ends of the span.

According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 for instructions.

> **Note** During the upgrade/downgrade some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSROSYNC, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure.
> A four-node BLSR can take up to five minutes to clear all of the BLSROSYNC alarms. Allow extra time for a large BLSR to clear all of the BLSROSYNC alarms.

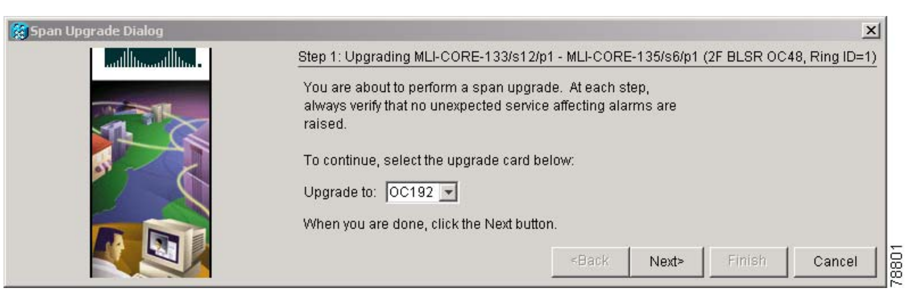
Step 4 In network view, right-click the span you want to upgrade.

Step 5 Choose **Span Upgrade** from the drop-down menu.

Step 6 The first Span Upgrade dialog box appears (Figure 14-1). Follow the instructions on the dialog box and the wizard will lead you through the rest of the span upgrade.

> **Note** The Back button is only enabled on Step 2 of the wizard; because you cannot back out of an upgrade via the wizard, close the wizard and initiate the manual procedure if you need to back out of the upgrade at any point beyond Step 2.

Figure 14-1 Span Upgrade Wizard



Caution As indicated by the wizard, when installing cards you must wait for the cards to boot up and become active before proceeding to the next step.

Note Remember to attach the fiber after installing the OC-N cards.

Note The span upgrade process resets the line's CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Step 7 Repeat Steps 4 through 6 for additional spans in the ring.

Stop. You have completed this procedure.

NTP-A95 Upgrade OC-N Spans Manually

Purpose	This procedure upgrades OC-N speeds within BLSRs, path protection, and 1+1 protection groups by upgrading OC-N cards. Complete a manual upgrade task if you need to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).
Tools/Equipment	Replacement cards
Prerequisite Procedures	The manual span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note OC-N card transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Note In this context the word "span" represents the OC-N path between two nodes. The words "span endpoint" represent the nodes on each end of a span.

Note If any of the cross-connect cards reboot during the span upgrade, you must reset each one when the span upgrade procedure is complete for all the nodes in the ring.

Step 1 Determine the type of span you need to upgrade and make sure you have the necessary cards. Valid span upgrades include:

- Four-port OC-3 to eight-port OC-3
- Single-port OC-12 to four-port OC-12
- Single-port OC-12 to OC-48
- Single-port OC-12 to OC-192
- OC-48 to OC-192

Caution You cannot upgrade a four-port OC-12 span. If the ring contains any OC-12-4 cards and you need to upgrade all the spans in the ring, you will need to downgrade the OC-12-4 card to a single-port OC-12 card (which is not possible unless only one port on the OC12-4 card is being used).

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 3.

Step 3 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 4 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present. See the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 for instructions.

Note During the upgrade/downgrade some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSROSYNC, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure.
A four-node BLSR can take up to five minutes to clear all of the BLSROSYNC alarms. Allow extra time for a large BLSR to clear all of the BLSROSYNC alarms. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for information about alarms.

Step 5 Complete the appropriate task:

- DLP-A293 Perform a Manual Span Upgrade on a Two-Fiber BLSR, page 14-13
- DLP-A294 Perform a Manual Span Upgrade on a Four-Fiber BLSR, page 14-14
- DLP-A295 Perform a Manual Span Upgrade on a Path Protection, page 14-16
- DLP-A296 Perform a Manual Span Upgrade on a 1+1 Protection Group, page 14-17
- DLP-A297 Perform a Manual Span Upgrade on an Unprotected Span, page 14-18

Note The span upgrade process resets the line's CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Note The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present; for example, no upgrade is possible from an OC48 span unless XC10G cards are installed in the nodes at both ends of the span.

Note A four-port OC-3 to eight-port OC-3 span upgrade, or an OC-12 to four-port OC-12 span upgrade can only be performed from multispeed slots (Slots 1 to 4 and 14 to17) because the OC3-8 and OC12-4 card can only be installed in multispeed slots. Ensure that the OC-3 and OC-12 cards are in multispeed slots before performing a span upgrade to the OC3-8 and OC12-4. The four OC-3 ports will be mapped to Ports 1-4 on the eight-port OC-3 card. The OC-12 port will be mapped to Port 1 on the four-port OC-12 card.

Stop. You have completed this procedure.

DLP-A293 Perform a Manual Span Upgrade on a Two-Fiber BLSR

Purpose	This task upgrades a two-fiber BLSR span to a higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48) which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19. To create circuits, see Chapter 8, "Create Circuits and VT Tunnels."

Step 1 Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 16-7.

Step 2 Remove the fiber from both endpoints and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both endpoints.

Step 4 From both endpoints, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit and receive signals fall within the acceptable range. See Table 2-5 on page 2-31 for OC-N card transmit and receive levels. If the receive level falls outside the acceptable range for that card, attenuate accordingly.

Step 9 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-37 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch from both endpoints on the upgraded span. See the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 16-8.

Step 11 Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task on page 6-24.

Step 12 Repeat this task for each span in the BLSR. When you are done with each span, the upgrade is complete.

Step 13 Return to your originating procedure (NTP).

DLP-A294 Perform a Manual Span Upgrade on a Four-Fiber BLSR

Purpose	This task upgrades a four-fiber BLSR span to a higher OC-N rate. Repeat the task to upgrade each span to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48) which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19. To create circuits, see Chapter 8, "Create Circuits and VT Tunnels."

Step 1 Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 16-7.

Step 2 Remove the fiber from both working and protect cards at both span endpoints (nodes) and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both end points.

Step 4 For both ends of the span endpoints, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-31 for OC-N card transmit and receive levels.

Step 9 Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-37 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch from both endpoints (nodes) on the upgraded span. See "DLP-A194 Clear a BLSR Force Ring Switch" task on page 16-8.

Step 11 Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task on page 6-24.

Step 12 Repeat these steps for each span in the BLSR. When all spans in the BLSR have been upgraded, the ring is upgraded.

Step 13 Return to your originating procedure (NTP).

DLP-A295 Perform a Manual Span Upgrade on a Path Protection

Purpose	This task upgrades path protection spans to a higher OC-N speed. Repeat the task for each span to upgrade the entire ring to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Do not perform any other maintenance operations or add any circuits during a span upgrade.

Step 1 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 16-16 to apply a Force switch on the span that you will upgrade.

Step 2 Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.

Step 3 Remove the OC-N cards from both span endpoints.

Step 4 For both ends of the span, in node view right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N card type.

Step 6 Click **OK**.

Step 7 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install the new OC-N cards in both endpoints.

Step 8 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-31 for OC-N card transmit and receive levels.

Step 9 Complete the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task on page 2-34 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 16-18 when cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared.

Step 11 Return to your originating procedure (NTP).

DLP-A296 Perform a Manual Span Upgrade on a 1+1 Protection Group

Purpose	This task upgrades a linear span to a higher OC-N rate. To downgrade a span, follow this task but choose a lower-rate card in Step 6.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Do not perform any other maintenance operations or add any circuits during a span upgrade.

Step 1 Initiate a Force switch on the ports you will upgrade, beginning with the protect port:

a. In node view, click the **Maintenance** > **Protection** tabs.

b. Choose the protection group from the Protection Groups area. In the Selected Group area, the working and protect spans appear.

c. In the Selected Group area, click the protect OC-N port.

d. In Switch Commands, choose **Force**.

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

FORCE-SWITCH-TO-WORKING appears next to the forced span.

Step 2 If you are upgrading a multiport card, repeat Step 1 for each port.

Step 3 Remove the fiber from both ends of the span and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both span endpoints.

Step 5 At both ends of the span, in node view, right-click the OC-N slot and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N card type.

Step 7 Click **OK**.

Step 8 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install the new OC-N cards in both endpoints.

Step 9 Verify that the transmit signal falls within the acceptable range. See Table 2-5 on page 2-31 for OC-N card transmit and receive levels.

Step 10 Complete the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task on page 2-33 to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 11 When cards on each end of the span have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the Force switch:

a. In node view, click the **Maintenance > Protection** tabs.

b. In the Protection Groups area, click the protection group that contains the card/port you want to clear.

c. In the Selected Group area, click the card you want to clear.

d. In Switch Commands, choose **Clear**.

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

Step 12 Repeat this task for any other spans in the 1+1 linear configuration.

Step 13 Return to your originating procedure (NTP).

DLP-A297 Perform a Manual Span Upgrade on an Unprotected Span

Purpose	This task manually upgrades unprotected spans to a higher OC-N rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 Upgrading unprotected spans will cause all traffic running on those spans to be lost.

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Caution Removing the fiber will cause all traffic on the unprotected span to be lost.

Step 1 Remove the fiber from both endpoint nodes in the span.

Step 2 Remove the OC-N cards from both span endpoints.

Step 3 For both ends of the span, in node view, right-click each OC-N slot and choose **Change Card**.

Step 4 In the Change Card dialog box, choose the new OC-N type.

Step 5 Click **OK**.

Step 6 When you have finished Steps 2 through 5 for both nodes, install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 7 Return to your originating procedure (NTP).

CHAPTER 15

Convert Network Configurations

This chapter explains how to convert from one SONET topology to another in a Cisco ONS 15454 network. For initial network turn up, see Chapter 6, “Turn Up Network.”

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.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A154 Convert a Point-to-Point to a Linear ADM, page 15-1—Complete as needed.
2. NTP-A155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR, page 15-3—Complete as needed.
3. NTP-A156 Convert a Point-to-Point or Linear ADM to a Path Protection, page 15-6—Complete as needed.
4. NTP-A210 Convert a Path Protectionto a Two-Fiber BLSR, page 15-7—Complete as needed.
5. NTP-A211 Convert a Two-Fiber BLSR to a Four-Fiber BLSR, page 15-9—Complete as needed.
6. NTP-A159 Modify a BLSR, page 15-11—Complete as needed.
7. NTP-A228 Manage BLSR Manual Ring Switches, page 15-12—Complete as needed.
8. NTP-A286 Convert DWDM Nodes to Hybrid Nodes, page 15-14—Complete as needed.

NTP-A154 Convert a Point-to-Point to a Linear ADM

Purpose	This procedure upgrades a point-to-point configuration (two nodes) to a linear add/drop multiplexer (ADM) configuration (three or more nodes).
Tools/Equipment	None
Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 6-3

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-5 on page 2-31.

Note In a point-to-point configuration, two OC-N cards are connected to two OC-N cards on a second node. The working OC-N ports have data communications channel (DCC) terminations, and the OC-N cards are in a 1+1 protection group.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the two point-to-point nodes. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 3 Log into the node that will be added to the point-to-point configuration (the new node).

Step 4 Complete the "NTP-A24 Verify Card Installation" procedure on page 4-2 to ensure that the new node has two OC-N cards with the same rate as the point-to-point nodes.

Step 5 Complete the "NTP-A35 Verify Node Turn Up" procedure on page 6-2 for the new node.

Step 6 Physically connect the fibers between the point-to-point node and the new node. The fiber connections should be connected working card to working card and protect card to protect card.

Step 7 On the new node, create a 1+1 protection group for the OC-N cards in the point-to-point node that will connect to the point-to-point node. See the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30.

Step 8 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for the working OC-N cards in the new node that will connect to the linear ADM network. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**.

Note DCC failure alarms appear until you create DCC terminations in the point-to-point node during Step 9.

Step 9 In node view display the point-to-point node that will connect to the new node.

Step 10 Complete the "NTP-A24 Verify Card Installation" procedure on page 4-2 to ensure that the point-to-point node has OC-N cards installed that can connect to the new node.

Step 11 Create a 1+1 protection group for the OC-N cards that will connect to the new node. See the "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 for instructions.

Step 12 Create DCC terminations on the working OC-N card that will connect to the new node. See the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4. In the Create SDCC Termination dialog box, set the port state to **IS**.

Step 13 From the view menu choose **Go to Node View** to open the new node in node view.

Step 14 Complete the "NTP-A28 Set Up Timing" procedure on page 4-22 for the new node. If the new node is using line timing, make the working OC-N card the timing source.

Step 15 From the view menu choose **Go to Network View**. Verify that the newly created linear ADM configuration is correct. One green span line should appear between each linear node.

Step 16 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 17 Repeat the procedure to add an additional node to the linear ADM.

Stop. You have completed this procedure.

DLP-A298 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**. Verify that all affected spans on the network map are green.

Step 2 Verify that the affected spans do not have active switches on the network map. Span ring switches are represented by the letters "L" for lockout ring, "F" for Force ring, "M" for Manual ring, and "E" for Exercise ring.

Step 3 A second verification method can be performed from the Conditions tab. Click **Retrieve Conditions** and verify that no switches are active. Make sure the Filter button is not selected.

Step 4 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 5 Return to your originating procedure (NTP).

NTP-A155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR

Purpose	This procedure upgrades a point-to-point configuration (two nodes) or a linear ADM configuration (three or more nodes) to a two-fiber bidirectional line switched ring (BLSR).
Tools/Equipment	None

Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 6-3 or NTP-A38 Provision a Linear ADM Network, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service affecting.

Note Optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-31.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the nodes that you want to convert from a point-to-point or ADM to a BLSR. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for each node in the configuration.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 4 On the network map right-click a span adjacent to the node you are logged into. A shortcut menu appears.

Step 5 From the shortcut menu, click **Circuits**. The Circuits on Span window appears.

Step 6 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

Note If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-192, no more than 96 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Caution If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to a BLSR. Refer to local procedures for relocating circuits if these requirements are not met.

Step 7 Repeat Steps 4 through 6 for each node in the point-to-point or linear ADM that you will convert to a BLSR. When all nodes comply with Step 6, proceed to the next step.

Step 8 For every node in the point-to-point or linear ADM network that you want to convert to a BLSR, complete the following tasks:

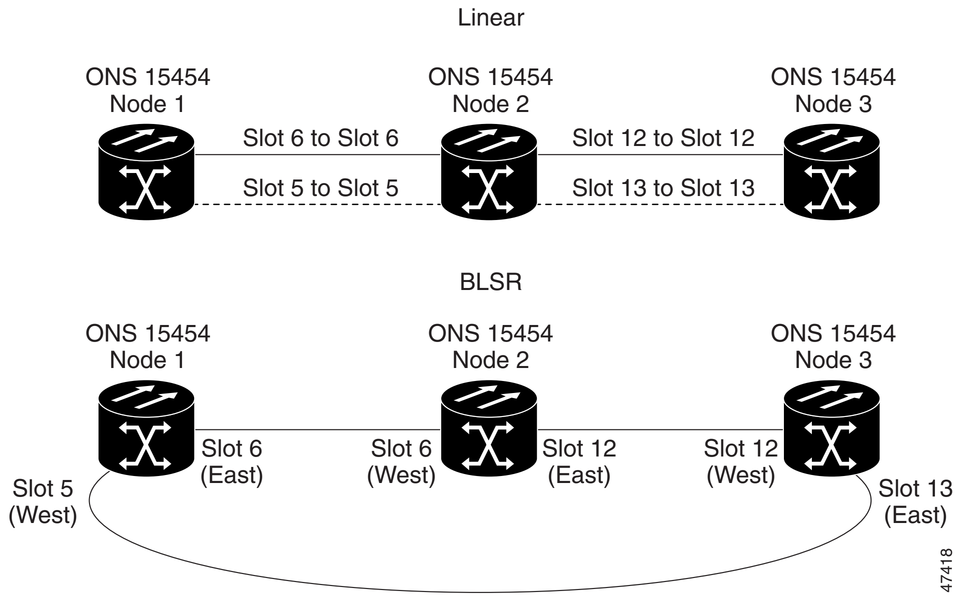
a. Complete the "DLP-A189 Verify that a 1+1 Working Slot is Active" task on page 15-6 for every 1+1 protection group that supports a span in the point-to-point or linear ADM network.

b. Complete the "DLP-A155 Delete a Protection Group" task on page 12-20 at each node that supports the point-to-point or linear ADM span.

c. Complete the "DLP-A214 Change the Service State for a Port" task on page 6-6 to put the protect ports out of service at each node that supports the point-to-point or linear ADM span.

Step 9 (Linear ADM only) Physically remove the protect fibers from all nodes in the linear ADM; for example, the fiber running from Node 2/Slot 13 to Node 3/Slot 13 (as shown in Figure 15-1) can be removed.

Figure 15-1 Linear ADM to BLSR Conversion



Step 10 Create the ring by connecting the protect fiber from one end node to the protect port on the other end node. For example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 (as shown in Figure 15-1) can be rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

Note If you need to remove any OC-N cards from the shelf do so now. In this example, cards in Node 2/Slots 5 and 13 can be removed. See the "NTP-A116 Remove and Replace a Card" procedure on page 2-57.

Step 11 From the network view, click the **Circuits** tabs and complete the "DLP-A516 Export CTC Data" task on page 9-4 to save the circuit data to a file on your hard drive.

Step 12 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 at the end nodes; provision the slot in each node that is not already in the SDCC Terminations list (in the Figure 15-1 example, Port 1 of Node 1/Slot 5 and Port 1 of Node 3/Slot 13).

Step 13 For circuits provisioned on an STS that is now part of the protection bandwidth (STSs 7 to 12 for an OC-12 BLSR, STSs 25 to 48 for an OC-48 BLSR, and STSs 97 to 192 for an OC-192 BLSR), delete and recreate each circuit:

a. Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 for one circuit.

b. Create the circuit on STSs 1 to 6 for an OC-12 BLSR, STSs 1 to 24 for an OC-48 BLSR, or STSs 1 to 96 for an OC-192 BLSR on the fiber that served as the protect fiber in the linear ADM. See the "NTP-A189 Create a Manually Routed OC-N Circuit" procedure on page 8-47 for instructions.

c. Repeat Steps a and b for each circuit residing on a BLSR protect STS.

Step 14 Complete the "NTP-A126 Create a BLSR" procedure on page 6-18 to put the nodes into a BLSR.

Stop. You have completed this procedure.

DLP-A189 Verify that a 1+1 Working Slot is Active

Purpose	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Selected Group area, verify that the working slot/port is shown as Working/Active. If so, this task is complete.

Step 3 If the working slot says Working/Standby, perform a Manual switch on the working slot:

a. In the Selected Group area, choose the Protect/Active slot.

a. In the Switch Commands field, choose **Manual**.

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

Step 4 Verify that the working slot is carrying traffic (Working/Active).

> **Note** If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 When the working slot is carrying traffic, clear the Manual switch:

a. In the Switch Commands field, choose **Clear**.

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

Step 6 Verify that the working slot does not revert to Standby, which might indicate a problem on the working span.

Step 7 Return to your originating procedure (NTP).

NTP-A156 Convert a Point-to-Point or Linear ADM to a Path Protection

Purpose	This procedure upgrades a point-to-point system to a path protection.
Tools/Equipment	None

Prerequisite Procedures	NTP-A124 Provision a Point-to-Point Network, page 6-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits are deleted and reprovisioned.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the point-to-point or linear ADM. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 3 Complete the "DLP-A189 Verify that a 1+1 Working Slot is Active" task on page 15-6 for each node.

Step 4 Complete the "DLP-A155 Delete a Protection Group" task on page 12-20 for each 1+1 protection group that supports the point-to-point or linear ADM span.

Step 5 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 at the protect cards in all nodes that will be part of the path protection.

Step 6 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18 and the "NTP-A188 Create an Automatically Routed OC-N Circuit" procedure on page 8-42 to delete and recreate the circuits one at a time.

Note If you want to add additional nodes to the path protection, see the "NTP-A105 Add a Path Protection Node" procedure on page 16-14.

Note A path protection is the default configuration if the cards installed are installed and the DCCs are configured.

Stop. You have completed this procedure.

NTP-A210 Convert a Path Protectionto a Two-Fiber BLSR

Purpose	This procedure converts a path protection to a two-fiber BLSR.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 6-36
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits on the ring are deleted and reprovisioned.

Caution Read through this procedure completely before beginning the conversion.

Note Prior to beginning this procedure, you should have a unique ring name to identify the new BLSR and a unique node ID number for each node on the ring.

Note Prior to beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-31.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node on the path protection. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 3 On the network map, right-click a span adjacent to the node you are logged into. A shortcut menu appears.

Step 4 From the shortcut menu, click **Circuits**. The Circuits on Span window appears.

Step 5 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

Note If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-192, no more than 96 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Caution If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.

Step 6 Repeat Steps 1 through 5 for each node in the path protection that you will convert to a BLSR. When all nodes comply with Step 5, continue with the next step.

Step 7 Save all circuit information:

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

b. Record the circuit information using one of the following options:

- From the File menu, click **Print** to print the circuits table. See the "DLP-A515 Print CTC Data" task on page 9-2 for more information.
- From the File menu, click **Export** and choose the data format: HTML, CSV (comma separated values), or TSV (tab separated values). Click **OK** and save the file in a temporary directory. See the "DLP-A516 Export CTC Data" task on page 9-4 for more information.

Step 8 Delete the circuits:

Note This method uses the network view. To delete circuits one at a time from each node, see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19.

a. In network view, click the **Circuits** tab. All circuits on the ring appear.

b. With the **Ctrl** key pressed, click each circuit. Each line turns dark blue as it is selected.

c. After all circuits have been selected, click **Delete**. Allow several minutes for processing; the actual length of time depends on the number of circuits in the network.

Step 9 Complete the "NTP-A126 Create a BLSR" procedure on page 6-18 to create the BLSR.

Step 10 To recreate the circuits, see Chapter 8, "Create Circuits and VT Tunnels" and choose the applicable procedure for the circuit type you want to enter.

Note To add additional nodes to a BLSR, see the "NTP-A212 Add a BLSR Node" procedure on page 16-1.

Stop. You have completed this procedure.

NTP-A211 Convert a Two-Fiber BLSR to a Four-Fiber BLSR

Purpose	This procedure upgrades a two-fiber BLSR to a four-fiber BLSR. The conversion will be easier if the same east and west configuration is used on all nodes being upgraded.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Two-fiber OC-48 or OC-192 BLSRs can be converted to four-fiber BLSRs. To convert, install two additional OC-48 or OC-192 cards at each two-fiber BLSR node, then log into CTC and convert the BLSR from two-fiber to four-fiber. The fibers that were divided into working and protect bandwidths for the two-fiber BLSR are now fully allocated for working BLSR traffic. A span upgrade can be performed prior to the two-fiber to four-fiber BLSR conversion.

Note BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the four-fiber BLSR and will have full BLSR protection. To route PCA circuits on protection channels in the four-fiber BLSR, delete and recreate the circuits after the upgrade. For example, if you upgrade a two-fiber OC-48 BLSR to four-fiber, PCA circuits on the protection STSs (STSs 25 to 48) in the two-fiber BLSR will remain in their existing STSs, which are working STSs in the four-fiber BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 1 to 24 in the protect bandwidth of the four-fiber BLSR. To delete circuits, see the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19. To create circuits, see Chapter 8, "Create Circuits and VT Tunnels."

Note Prior to beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in Table 2-5 on page 2-31.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at one of the two-fiber nodes that you want to convert.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 3 Complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install two OC-48 or OC-192 cards at each BLSR node. You must install the same OC-N card rate as the two-fiber BLSR.

Step 4 Connect the fiber to the new cards. Use the same east-west connection scheme that was used to create the two-fiber connections. See the "NTP-A247 Install Fiber-Optic Cables on OC-N Cards" procedure on page 2-29.

Step 5 Complete the "DLP-A214 Change the Service State for a Port" task on page 6-6 to enable (put in service) the ports for each new OC-N card.

Step 6 Test the new fiber connections using procedures standard for your site.

Step 7 Convert the BLSR:

a. Display the network view and click the **Provisioning > BLSR** tabs.

b. Choose the two-fiber BLSR you want to convert then click **the Upgrade to 4 Fiber** button.

c. In the Upgrade BLSR dialog box, set the amount of time that will pass before the traffic reverts to the original working path after the condition that caused the switch has been resolved. The default is 5 minutes.

d. Click **Next**.

e. Assign the east and west protection ports:

   - West Protect—Select the west BLSR port that will connect to the west protect fiber from the drop-down menu.
   - East Protect—Select the east BLSR port that will connect to the east protect fiber from the drop-down menu.

f. Click **Finish**.

Step 8 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 9 Complete the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 6-30.

Stop. You have completed this procedure.

NTP-A159 Modify a BLSR

Purpose	This procedure changes a BLSR ring name, node ID, or ring and span reversion times.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node in the BLSR you want to modify. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

> **Note** Some or all of the following alarms appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC. The alarms clear after you configure all the nodes in the BLSR. For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 To change the BLSR ring name or the ring or span reversion times, complete the following steps. If you want to change a node ID, continue with Step 4.

a. In network view, click the **Provisioning > BLSR** tabs.

b. Click the BLSR you want to modify and click **Edit**.

c. In the BLSR window, change any of the following:

   - Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. The alphanumeric character strings that can be used are 0 to 9 and A to Z. You can combine numbers and letters and use upper or lower case letters. Do not use the character string "All" in either upper or lower case letters because it is a TL1 keyword. Do not choose a name that is already assigned to another BLSR.
   - Reversion time—If needed, change the amount of time that will pass before the traffic reverts to the original working path after a ring switch.
   - Span Reversion—(Four-fiber BLSRs only) If needed, change the amount of time that will pass before the traffic reverts to the original working path after a span switch.

d. Click **Apply**.

If you changed the ring name, the BLSR window closes automatically. If you only changed a reversion time, close the window by choosing **Close** from the File menu.

Step 4 As needed complete the "DLP-A326 Change a BLSR Node ID" task on page 15-12; otherwise, continue with Step 5.

Step 5 In network view, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, BLSROSYNC, and Node ID Mismatch alarms are cleared.

Note For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Stop. You have completed this procedure.

DLP-A326 Change a BLSR Node ID

Purpose	This task changes a BLSR node ID.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 On the network map, double-click the node with the node ID you want to change.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Choose a Node ID number. Do not choose a number already assigned to another node in the same BLSR.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

NTP-A228 Manage BLSR Manual Ring Switches

Purpose	This procedure initiates or clears a BLSR Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node in the BLSR you want to modify. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-A301 Initiate a BLSR Manual Ring Switch" task on page 15-13.

Step 3 As needed, complete the "DLP-A241 Clear a BLSR Manual Ring Switch" task on page 15-13.

Stop. You have completed this procedure.

DLP-A301 Initiate a BLSR Manual Ring Switch

Purpose	This task performs a BLSR Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon and drag and drop it in a new location.

Step 4 Right-click any BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Note 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. Right-click either working port.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Step 7 Verify that the channel (port) displays the letter "M" for Manual ring. Also verify that the span lines between the nodes where the Manual switch was invoked turn purple, and that the span lines between all other nodes turn green on the network view map. This confirms the Manual switch.

Step 8 From the File menu, choose **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-A241 Clear a BLSR Manual Ring Switch

Purpose	This task clears a Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon on the Edit BLSR network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click the BLSR node channel (port) where the Manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 In the dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** on the Confirm BLSR Operation dialog box. The letter "M" is removed from the channel (port) and the span turns green on the network view map.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

NTP-A286 Convert DWDM Nodes to Hybrid Nodes

Purpose	This procedure upgrades an OSCM card to an OSC-CSM card. OSCM cards use Slots 8 and 10 which are required for cross-connect cards in TDM and DWDM hybrid configurations. The OSC-CSM cards use Slots 1 to 6 and 12 to 17.
Tools/Equipment	Two OSC-CSM cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note This is an in-service procedure and is not traffic affecting.

Note This procedure only applies to the OSCM cards that are installed in nodes running Software Release 4.6. You cannot perform this upgrade on software released prior to Software R4.6.

Note Downgrade procedures from OSC-CSM cards to OSCM cards are not supported. Contact Cisco Technical Assistance Center (TAC) for more information Contact Cisco Technical Assistance Center (TAC) for more information, see the "Obtaining Technical Assistance" section on page lviii.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.

Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7.

Step 3 If you have timing set up on the OSCM card, delete the timing source:

a. In node view, click the **Provisioning > Timing tabs.**

b. Scroll down to the Reference Lists pane.

c. In the NE Reference column, select **Internal Clock** from the drop-down menu for all entries where the selected Clock Source is the OSCM that you are removing.

d. Click **Apply**.

Step 4 If you have overhead circuits on the node, complete the "DLP-A334 Delete Overhead Circuits" task on page 11-21.

Step 5 Delete the DWDM ring ID:

a. In node view, click the **Provisioning > DCC/GCC/OSC > OSC** tabs.

b. Select the DWDM Ring ID you want to delete and click **Delete**.

c. In the Delete DWDM Ring ID confirmation box, click **Yes**. Confirm that the changes appear.

Step 6 If you have OSC terminations, complete the "DLP-A361 Delete a DWDM OSC Termination" task on page 12-22.

Step 7 Delete the OSCM card WDM-ANS connections:

a. In node view, click the **Provisioning > WDM-ANS > Connections** tabs.

b. Select the connection to be deleted.

c. Click **Delete**.

d. From the Delete Optical Link dialog box, click **Yes**.

Step 8 Delete the card from CTC:

a. In node view, right-click the OSCM card.

b. Select **Delete Card** from the menu.

The card name disappears and the slot turns gray.

Step 9 Remove cables from the OSCM OSC ports.

Step 10 Physically replace the deleted OSCM card on the ONS 15454 with an OSC-CSM card:

Note The OSCM card and OSC-CSM card do not have the same slot requirements.

a. Open the OSCM card ejectors.

b. Slide the card out of Slots 8 or 10.

c. Open the ejectors on the OSC-CSM card.

d. Slide the OSC-CSM card into the slot along the guide rails. Use Slots 1 to 6 or 12 to 17 according to your site plan.

e. Close the ejectors.

Note On the OSC-CSM card the fail LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The ACT/STBY LED turns green and remains on. In node view, the OSC-CSM appears green.

Step 11 If an OSCM card was removed from Slot 8 and an OSC-CSM card was installed in Slots 12—17, modify the OSC-CSM line direction from east-to-west to west-to-east.

Note The MetroPlanner configuration file will label the OSC-CSM card as west even if it is installed in the east-side of the node.

a. To modify OSC-CSM card line direction, double-click the OSC-CSM card from node view.
b. Click the **Provisioning > Optical Line > Parameter** tabs.
c. In the port number 2 line, click the Line Direction drop-down menu and choose **West to East**.
d. Click **Apply**.

Step 12 If an OSCM card was removed from Slot 10 and an OSC-CSM card was installed in Slots 1—6, modify the OSC-CSM line direction from west-to-east to east-to-west.

Note The MetroPlanner configuration file will label the OSC-CSM card as east even if it is installed in the west-side of the node.

a. To modify OSC-CSM card line direction, double-click the OSC-CSM card in node view.
   The card view opens.
b. Click the **Provisioning > Optical Line > Parameter** tabs.
c. In the port number 2 line, click the Line Direction drop-down menu and choose **East to West**.
d. Click **Apply**.

Step 13 Calculate default connections using WDM-ANS:

a. Click the CTC up arrow to get back to node view.
b. In node view, click the **Provisioning > WDM-ANS > Connections** tabs.
c. Click the **Calculate Connections** button.

Step 14 Connect the cables from the OSC-CSM LINE ports to the OPT-BST OSC ports. Follow the recommended connections that were automatically calculated in the **Connections** tab described in Step 13.

Step 15 Launch ANS port regulation:

a. In node view, click the **Provisioning > WDM-ANS > Port Status** tabs.
b. Click the **Launch ANS** button.
c. In the Link Status column the ports change to Regulated.

Step 16 Create OSC terminations starting from the OSC-CSM card. Complete the "DLP-A342 Provision OSC Terminations" task on page 5-11.

Step 17 Complete "DLP-A345 Provision the Ring ID" task on page 7-9.

Step 18 (Optional) If you want to set up timing on the OSC-CSM card, create the timing source:

a. In node view, click the **Provisioning > Timing tabs.**

b. Scroll down to the Reference Lists pane.

c. In the NE Reference column, select **Internal Clock** from the drop-down menu for all entries where the selected Clock Source is the OSCM that you are adding.

d. Click **Apply**.

Step 19 (Optional) Complete the "NTP-A194 Create Overhead Circuits" procedure on page 8-93.

Step 20 Repeat Steps 3 through 19 for each OSCM card you are replacing in the node.

Step 21 If you are installing cross-connect cards, complete the "DLP-A37 Install the XC, XCVT, or XC10G Cards" task on page 2-9.

Stop. You have completed this procedure.

Add and Remove Nodes

This chapter explains how to add and remove Cisco ONS 15454 nodes from bidirectional line switched rings (BLSRs), path protection, and linear add/drop multiplexers (ADMs).

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.

Before You Begin

Before performing any of the following procedures, complete the "NTP-A195 Document Existing Provisioning" procedure on page 9-2. Also investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-A212 Add a BLSR Node, page 16-1—Complete as needed.
2. NTP-A213 Remove a BLSR Node, page 16-9—Complete as needed.
3. NTP-A105 Add a Path Protection Node, page 16-14—Complete as needed.
4. NTP-A106 Remove a Path Protection Node, page 16-18—Complete as needed.
5. NTP-A262 Add a Node to a Linear ADM, page 16-19—Complete as needed.
6. NTP-A263 Remove a Node from a Linear ADM, page 16-21—Complete as needed.

NTP-A212 Add a BLSR Node

Purpose	This procedure expands a BLSR by adding a node.
Tools/Equipment	Fiber for new node connections
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the BLSR. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up Node."
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Adding a BLSR node can be service affecting and should be performed during a maintenance window.

Step 1 Draw a diagram of the BLSR where you will add the node. In the diagram, identify the east and west BLSR OC-N trunk (span) cards that will connect to the new node. This information is essential to complete this procedure without error. Figure 16-1 shows a drawing of a three-node, two-fiber BLSR that uses Slots 5 and 12 for the BLSR trunk cards. The dashed arrow shows the new fiber connections that will be made to add the fourth node to the BLSR.

Figure 16-1 Three-Node, Two-Fiber BLSR Before a Fourth Node Is Added

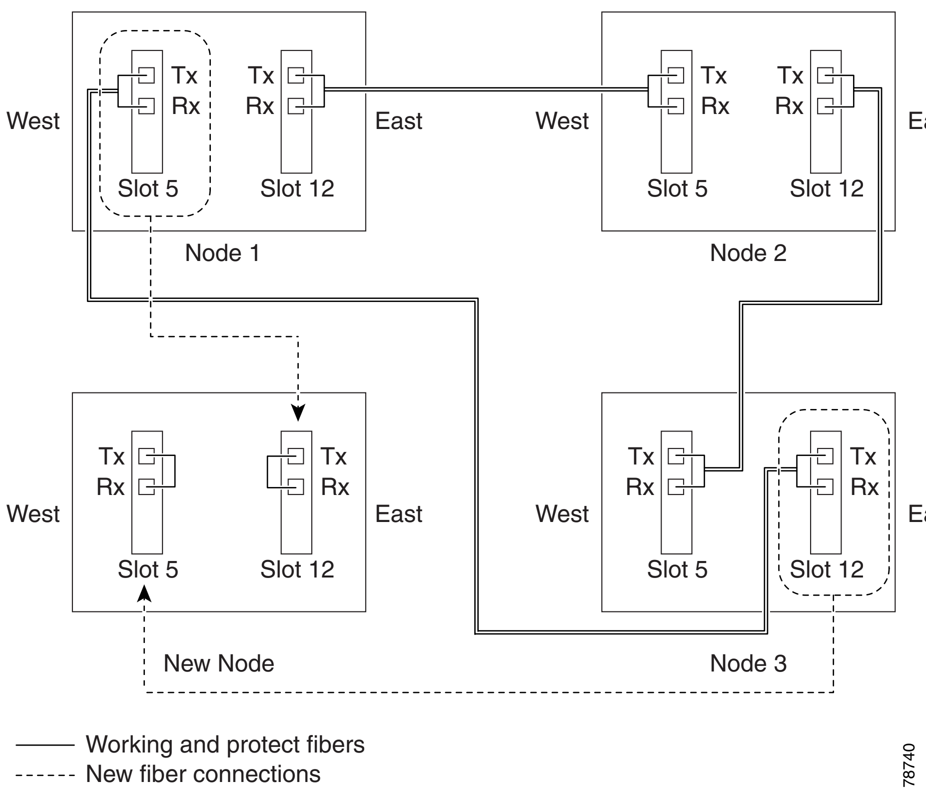
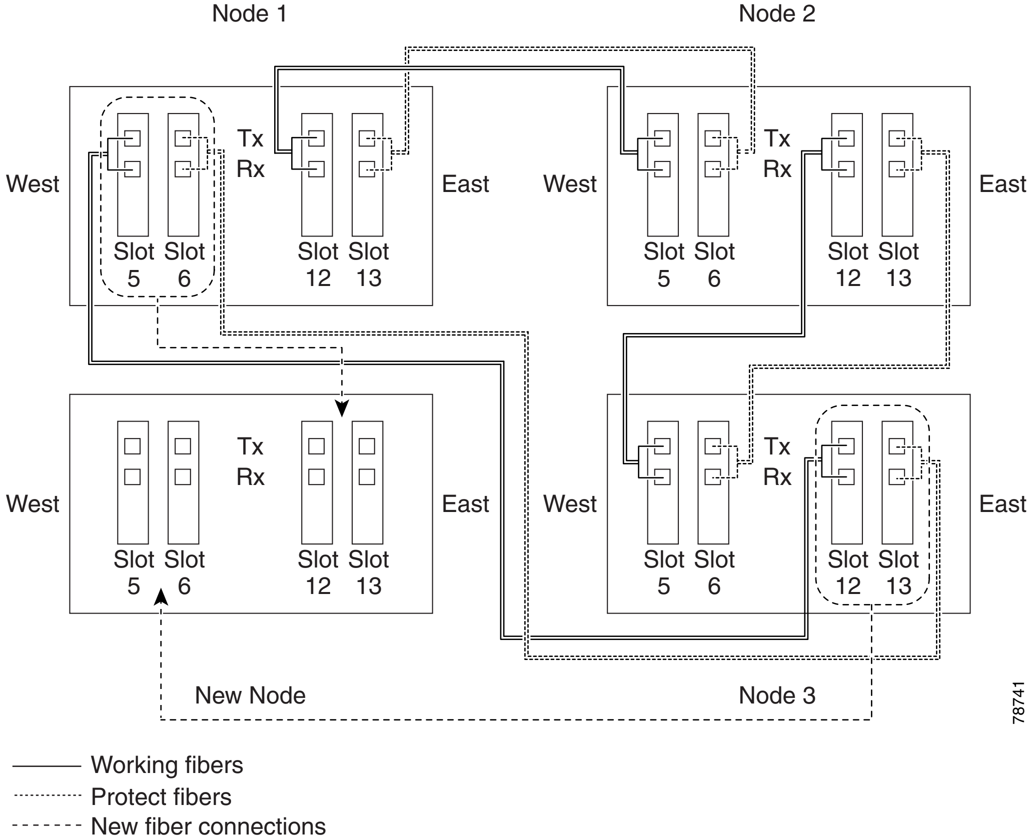


Figure 16-2 shows a sample drawing of a four-fiber BLSR. The dashed arrow shows the new fiber connections that will be made to add the fourth node. For four-fiber BLSRs, two fiber sets will be reconnected, the working fiber and the protect fiber.

Figure 16-2 Three-Node, Four-Fiber BLSR Before a Fourth Node is Added



Step 2 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for all the nodes in the ring.

Step 3 Verify the card installation on the new node using the "NTP-A24 Verify Card Installation" procedure on page 4-2. Verify that the OC-N cards that will be the BLSR trunk cards match the BLSR optical rate. For example, if the BLSR is OC-48, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the optical rates do not match the BLSR, complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12.

Step 4 Verify that fiber is available to connect the new node to the existing nodes. Refer to the diagram drawn in Step 1.

Step 5 Complete the "NTP-A35 Verify Node Turn Up" procedure on page 6-2. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 6 Create a static route on the new node if the following conditions are present. If the conditions are not present, continue with Step 7.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the new node Provisioning > Network > General subtab, Craft Access Only is not checked under Gateway Settings.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If these conditions are present, add static routes on the node that will be added to the BLSR, using the following settings:

- Destination IP address: *IP-address-of-the-CTC-computer-connected-to-the-new-node*
- Net Mask: **255.255.255.255**
- Next Hop: *IP-address-of-the-Cisco-ONS-15454*
- Cost: **1**

See the "DLP-A65 Create a Static Route" task on page 4-15. To view Gateway Settings, see the "DLP-A249 Provision IP Settings" task on page 4-10.

Step 7 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a node in the BLSR.

Step 8 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that the BLSR is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 9 From the View menu, choose **Go to Network View** and click the **Provisioning > BLSR** tabs.

Step 10 On paper, record the Ring Name, Ring Type, Line Rate, Ring Reversion, and Span Reversion (4 Fiber).

Step 11 From the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Step 12 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-A60 Log into CTC" task on page 3-24.

Step 13 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15454 Troubleshooting Guide*, as necessary.

Step 14 Using the information recorded in Steps 10 and 11 and the diagram created in Step 1, create a BLSR on the new node. See the "DLP-A242 Create a BLSR on a Single Node" task on page 16-6.

Step 15 (Optional) Create test circuits, making sure they pass through the BLSR trunk cards, and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-A189 Create a Manually Routed OC-N Circuit" procedure on page 8-47 and the "NTP-A62 Test OC-N Circuits" procedure on page 8-54 for information.

Step 16 Create the data communications channel (DCC) terminations on the new node. See the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4.

Note Creating the DCC terminations causes the SDCC Termination Failure and Loss of Signal alarms to appear. These alarms remains active until you connect the node to the BLSR.

Note If you map the K3 byte to another byte (such as E2), you must remap the line cards on either side of the new node to the same byte. See the "DLP-A89 Remap the K3 Byte" task on page 6-18.

Step 17 Complete the "DLP-A60 Log into CTC" task on page 3-24 at a BLSR node that will connect to the new node.

Step 18 Referring to the diagram created in Step 1, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 16-7 on the node that will connect to the new node on its west line (port). In the Figure 16-2 example, the BLSR force ring would occur at Node 1, West line (Slot 5 and 6).

Step 19 Referring to the diagram created in Step 1, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 16-7 on the node that will connect to the new node on its east line (port). In the Figure 16-2 example, the BLSR force ring would occur at Node 3, East line (Slot 12 and 13).

Step 20 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 21 Following the diagram created in Step 1, remove the fiber connections from the two nodes that will connect to the new node.

a. Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 16-1 example, this is Node 1, Slot 5, and in Figure 16-2 this is Node 1, Slots 5 and 6.

b. Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 16-1 example, this is Node 3, Slot 12, and in Figure 16-2 this is Node 3, Slots 12 and 13.

Step 22 Connect fibers from the adjacent nodes to the new node following the diagram created in Step 1. Connect the west port to the east port and the east port to the west port. For four-fiber BLSRs, connect the protect fibers.

Step 23 After the newly added node appears in network view, double-click it to display the node in node view.

Step 24 Click the **Provisioning > BLSR** tabs.

Step 25 Click **Ring Map**. Verify that the new node appears on the Ring Map with the other BLSR nodes, then click **OK**.

Step 26 From the View menu, choose **Go to Network View** and check the following:

a. Click the **Provisioning > BLSR** tabs. Verify that the new node appears under the Node column.

b. Click the **Alarms** tab. Verify that BLSR alarms such as RING MISMATCH, E-W MISMATCH, PRC-DUPID (duplicate node ID), and APSCDFLTK (default K) do not appear.

If the new node does not appear in the Node column, or if BLSR alarms are present, log into the new node and verify that the BLSR is provisioned on it correctly with the information from Steps 10 and 11. If the node still does not appear, or if alarms persist, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 27 Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node will be shown as incomplete.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 28 In network view, right-click the new node and choose **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits in the dialog box is correct.

Step 29 If incomplete circuits are still present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 30 Click the **History** tab. Verify that BLSR_RESYNC conditions appear for every node in the BLSR.

Step 31 Complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 16-8 to remove the ring switch from the east and west BLSR lines.

Step 32 According to local site practice, complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 6-22 or the "NTP-A176 Four-Fiber BLSR Acceptance Test" procedure on page 6-30.

Stop. You have completed this procedure.

DLP-A242 Create a BLSR on a Single Node

Purpose	This task creates a BLSR on a single node. Use it to add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 In the Suggestion dialog box, click **OK**.

Step 3 In the Create BLSR dialog box, enter the BLSR information:

- Ring Type—Enter the ring type (either 2 Fiber or 4 Fiber) of the BLSR.
- Ring Name—Enter the BLSR ring name. If the node is being added to a BLSR, use the BLSR ring name.
- Node ID—Enter the node ID. If the node is being added to a BLSR, use an ID that is not used by other BLSR nodes.
- Ring Reversion—Enter the ring reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR via the node's west line (port).
- East Line—Enter the slot on the node that will connect to the existing BLSR via the node's east line (port).

If you are adding the node to a four-fiber BLSR, complete the following for the second set of fibers:

- Span Reversion—Enter the span reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR via the node's west line.
- East Line—Enter the slot on the node that will connect to the existing BLSR via the node's east line.

Step 4 Click **OK**.

Note The BLSR is incomplete and alarms are present until the node is connected to other BLSR nodes.

Step 5 Return to your originating procedure (NTP).

DLP-A303 Initiate a BLSR Force Ring Switch

Purpose	Use this task to perform a BLSR Force switch on a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**.

Step 4 To apply a Force switch to the west line:

a. Right-click the west BLSR port where you want to switch the BLSR traffic and choose **Set West Protection Operation**.

> **Note** If node icons overlap, drag and drop the icons to a new location. You can also return to network view and change the positions of the network node icons, because BLSR node icons are based on the network view node icon positions.

> **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. Right-click either working port.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the pull-down menu. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 5 To apply a Force switch to the east line:

a. Right-click the east BLSR port and choose **Set East Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons, since BLSR node icons are based on the network view node icon positions.

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. Right-click either working port.

---

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the pull-down menu. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-A194 Clear a BLSR Force Ring Switch

Purpose	This task removes a Force switch from a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**.

Step 4 To clear a Force switch on the west line:

a. Right-click the BLSR west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

Step 5 To clear a Force switch on the east line:

a. Right-click the BLSR east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

On the BLSR network graphic, a green and a purple span line connects each node. This is the normal display for BLSRs when protection operations are not invoked.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

NTP-A213 Remove a BLSR Node

Purpose	This procedure removes a node from a BLSR.
Tools/Equipment	None
Prerequisite Procedures	NTP-A126 Create a BLSR, page 6-18
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals. You will delete all circuits that originate and terminate on the node that will be removed. In addition, you will verify that circuits passing through the node do not enter and exit the node on different STSs and/or VTs. If they do, you will delete and recreate the circuits, and traffic will be lost during this time.

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for all the nodes in the ring.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node that you are going to remove from the BLSR.

Step 3 Complete the "DLP-A195 Verify Timing in a Reduced Ring" task on page 16-11.

Note If you remove a node that is the only building integrated timing supply (BITS) for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect traffic performance.

Step 4 Create a diagram of the BLSR where you will remove the node. You can draw the BLSR manually, or print it from CTC by performing the following steps:

a. From the View menu, choose **Go to Network View**.

b. Click the **Provisioning** > **BLSR** tab, click the BLSR, then click **Edit**.

c. In the BLSR window, verify that all the port information is visible. If not, press **Ctrl** and drag the node icons to a new location so the information can be viewed.

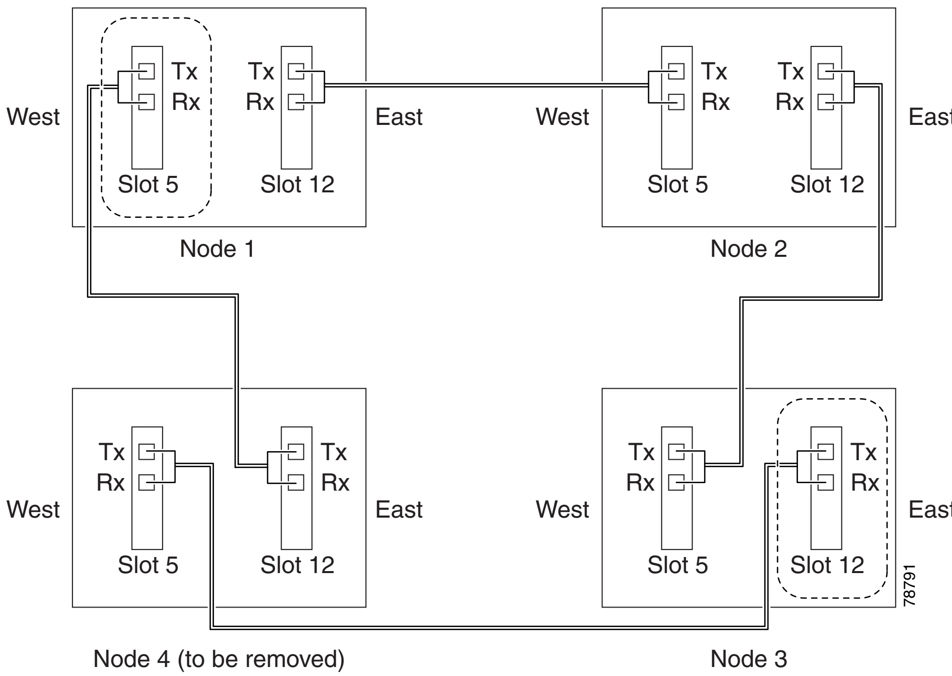
d. Complete the "DLP-A515 Print CTC Data" task on page 9-2.

e. Close the BLSR window by choosing **Close** from the File menu.

Step 5 Referring to the BLSR diagram, identify the following:

- The node that is connected via its west port to the target (removal) node. For example, if you were removing Node 4 in Figure 16-3, Node 1 is the node connected via its west port to Node 4.
- The node that is connected via its east port to the target (removal) node. In Figure 16-3, Node 3 is the node connected via its east port to Node 4.

Figure 16-3 Four-Node, Two-Fiber BLSR Before a Node Is Removed



Step 6 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that the BLSR is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 7 From the View menu, choose **Go to Other Node**. Choose the node that you will remove and click **OK**.

Step 8 Click the **Circuits** tab. If the Scope setting is set to Network, choose **Node** from the Scope pull-down menu. Make sure that the Filter button is off (not indented) to ensure that all circuits are visible.

Step 9 Delete all circuits that originate or terminate on the node. See the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18.

Step 10 Complete the "DLP-A304 Verify Pass-Through Circuits" task on page 16-12 to verify that circuits passing through the target node enter and exit the node on the same STS and/or VT.

Step 11 From the View menu, choose **Go to Network View**.

Step 12 Referring to the diagram created in Step 4, complete the "DLP-A303 Initiate a BLSR Force Ring Switch" task on page 16-7 at each node that connects to the target (removal) node to force traffic away from it. You must perform a Force switch at each port connected to the target node. For example, in Figure 16-3, you would perform a Force switch on the east port of Node 3 and the west port of Node 1.

Step 13 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task on page 9-32 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.

Step 14 Remove the fiber connections between the node being removed and the two neighboring nodes.

Step 15 If the two nodes that will be connected after the BLSR node is removed have OC-48 AS trunk (span) cards and their K3 bytes were remapped, complete the "DLP-A422 Verify BLSR Extension Byte Mapping" task on page 16-13. If not, continue with Step 16.

Step 16 Reconnect the fiber of the two neighboring nodes directly, west port to east port. For example, in Figure 16-3, the east port of Node 3 (Slot 12) connects to the west port of Node 1 (Slot 5).

Step 17 If you do not plan to add the removed node to a BLSR in the future, complete the "DLP-A196 Delete a BLSR from a Single Node" task on page 16-14. If you will add the node to a BLSR in the future, go to Step 18.

Step 18 If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. (Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group.) Delete the node from the login node group:

a. From the CTC Edit menu, choose **Preferences**.

b. In the Preferences dialog box, click the **Login Node Groups** tab.

c. Click the login node group tab containing the node you want to remove.

d. Click the node you want to remove, then click **Remove**.

e. Click **OK**.

Step 19 Click the **History** tab. Verify that the BLSR_RESYNC condition appears for every node in the BLSR.

Step 20 Complete the "DLP-A194 Clear a BLSR Force Ring Switch" task on page 16-8 to remove the Force protection switches.

Step 21 According to local site practice, complete the "NTP-A175 Two-Fiber BLSR Acceptance Test" procedure on page 6-22.

Stop. You have completed this procedure.

DLP-A195 Verify Timing in a Reduced Ring

Purpose	This task verifies timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite/remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Observe the Timing Mode field to see the type of timing (Line, External, Mixed) that has been set for that node.

Step 3 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the only BITS timing source, perform the following:

a. Contact your synchronization coordinator or appropriate personnel before continuing with this procedure.

b. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-A157 Change the Node Timing Source" task on page 12-23.

c. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set that node's Timing Mode to **External**, set BITS-1 and BITS-2 BITS In State to **OOS**, and set the NE Reference to **Internal**. Then, choose line timing for all other nodes in the ring. This forces the first node to be their primary timing source. (See the "DLP-A157 Change the Node Timing Source" task on page 12-23.)

Note This type of timing conforms to Stratum 3 requirements and is not considered optimal.

Step 5 If the removed node was not the only BITS timing source, provision the adjacent nodes to line timing using SONET links (east and west) as timing sources, traceable to the node with external BITS timing. See the "NTP-A28 Set Up Timing" procedure on page 4-22.

Step 6 Return to your originating procedure (NTP).

DLP-A304 Verify Pass-Through Circuits

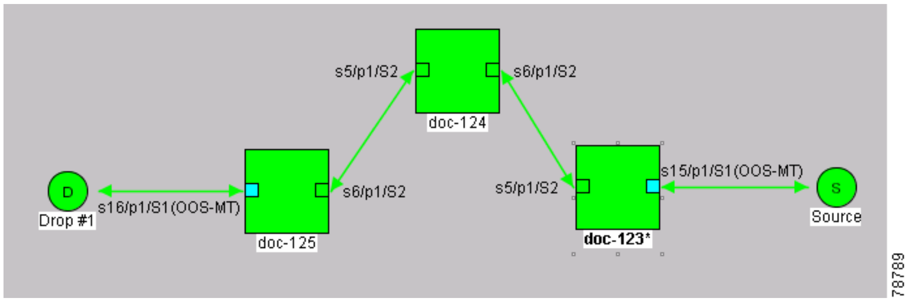
Purpose	This task verifies that circuits passing through a BLSR or path protection node enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the CTC Circuits window, choose a circuit that passes through the BLSR or path protection node that will be removed and click **Edit**.

Step 2 In the Edit Circuits window, check **Show Detailed Map**.

Step 3 Verify that the STS and VT mapping on the node's east and west ports are the same. For example, if the circuit mapping on the west port is s5/p1/S1 (Slot 5, Port 1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit displays different STSs and/or VTs on the east and west ports, write down the name of the circuit. Figure 16-4 shows a circuit passing through a node (doc-124) on the same STS (STS 2).

Figure 16-4 Verifying Pass-Through STSs



Step 4 Repeat Steps 1 to 3 for each circuit in the Circuits tab.

Step 5 Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different STSs. To delete the circuit, see the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" task on page 11-18. To create the circuit, see Chapter 8, "Create Circuits and VT Tunnels."

Step 6 Return to your originating procedure (NTP).

DLP-A422 Verify BLSR Extension Byte Mapping

Purpose	This task verifies that the extension byte mapping is the same on BLSR trunk (span) cards that will be connected after a node is removed from a BLSR.
Tools/Equipment	OC-48 AS cards must be installed at one or both ends of the BLSR span that will be connected.
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, double-click a BLSR node with OC-48 AS trunk (span) cards that will be reconnected after a BLSR node removal.

Step 2 Double-click one OC-48 AS BLSR trunk card.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Record on paper the byte in the BLSR Ext Byte column.

Step 5 Repeat Steps 2 through 4 for the second OC-48 AS trunk card.

Step 6 If the node at the other end of the new span contains OC-48 AS trunk cards, repeat Steps 1 through 5 at the node. If it does not have OC-48 AS cards, their trunk cards are mapped to the K3 extension byte. Continue with Step 7.

Step 7 If the trunk cards on each end of the new span are mapped to the same BLSR extension byte, continue with Step 8. If they are not the same, remap the extension byte of the trunk cards at one of the nodes. See the "DLP-A89 Remap the K3 Byte" task on page 6-18.

Step 8 Return to your originating procedure (NTP).

DLP-A196 Delete a BLSR from a Single Node

Purpose	This task deletes a BLSR from a node after you remove the node from the BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the BLSR:

- If the node that was removed is connected to the same LAN as your computer, from the File menu, choose **Add Node**, then enter the node name or IP address.
- If the node that was removed is not connected to the same LAN as your computer, you must connect to the node using a direct connection. See Chapter 3, "Connect the PC and Log into the GUI" for procedures.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Highlight the ring and click **Delete**.

Step 4 In the Suggestion dialog box, click **OK**.

Step 5 In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 6 Return to your originating procedure (NTP).

NTP-A105 Add a Path Protection Node

Purpose	This procedure adds a node to a Path Protection.
Tools/Equipment	None
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the Path Protection. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up Node." NTP-A44 Provision Path Protection Nodes, page 6-36
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for all the nodes in the ring.

Step 2 Log into an existing node in the path protection where you want to add a node. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that the path protection is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15454 Troubleshooting Guide*, as necessary.

Step 4 Verify the card installation on the new node. See the "NTP-A24 Verify Card Installation" procedure on page 4-2. Check that the OC-N cards that will serve as the path protection trunk (span) cards match the path protection optical rate of the trunk cards to which the new node will be connected. For example, if the adjacent nodes have OC-48 trunk cards, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the rate does not match the rate of the adjacent node trunk cards, complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12 to install them.

Step 5 Verify that fiber is available to connect the new node to the existing nodes.

Step 6 Complete the "NTP-A35 Verify Node Turn Up" procedure on page 6-2.

Step 7 Determine if the following conditions are present.

- The IP address for the new node is on the same subnet as other nodes in the network.
- On the new node Provisioning > Network > General subtab, Craft Access Only is not checked under Gateway Settings.
- A CTC computer is directly connected to the new node.
- CTC computers are directly connected to other nodes on the same subnet.

If the conditions are not present, continue with Step 8. If conditions are present, complete the "DLP-A65 Create a Static Route" task on page 4-15 on the node that will be added to the path protection. Use the following settings:

- Destination IP address: *IP address of the CTC computer connected to the new node*
- Net Mask: **255.255.255.255**
- Next Hop: *IP address of the Cisco ONS 15454*
- Cost: **1**

To view Gateway Settings, see the "DLP-A249 Provision IP Settings" task on page 4-10.

Step 8 Log into the new node:

- If the node has a LAN connection and appears on the network map, from the View menu, choose **Go to Other Node**, then enter the new node.
- If the new node is not connected to the network, log into it using the "DLP-A60 Log into CTC" task on page 3-24.

Step 9 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See the *Cisco ONS 15454 Troubleshooting Guide*, as necessary.

Step 10 (Optional) Create test circuits, making sure they pass through the path protection trunk cards, and run test traffic through the node to ensure that the cards are functioning properly. See the "NTP-A189 Create a Manually Routed OC-N Circuit" procedure on page 8-47 and the "NTP-A62 Test OC-N Circuits" procedure on page 8-54 for information.

Step 11 Create the DCC terminations on the new node. See the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4.

Step 12 From the View menu, choose **Go to Network View**.

Step 13 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 16-16 to switch traffic away from the span that will be broken to connect to the new node.

Step 14 Two nodes will connect directly to the new node; remove their fiber connections:

a. Remove the east fiber connection from the node that will connect to the west port of the new node.

b. Remove the west fiber connection from the node that will connect to the east port of the new node.

Step 15 Replace the removed fibers with the fibers that are connected to the new node.

Step 16 Log out of CTC and log back into a node in the network.

Step 17 From the View menu, choose **Go to Network View** to display the path protection nodes. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.

Step 18 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Count the number of incomplete circuits.

Note UNEQ-P alarms may appear on the nodes in your network, this is normal, and the alarms will clear after the circuits are updated.

Step 19 In the network view, right-click the new node and choose **Update Circuits With New Node** from the shortcut menu. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits in the dialog box is correct.

Step 20 Click the **Circuits** tab and verify that no incomplete circuits are present.

Note If the circuits take more than a minute to appear, log out of CTC, then log back in.

Step 21 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 16-18 to clear the protection switch.

Step 22 According to local site practice, complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38.

Stop. You have completed this procedure.

DLP-A197 Initiate a Path Protection Force Switch

Purpose	This task switches all circuits on a path protection span to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the span where you want to switch path protection traffic away. Choose **Circuits** from the shortcut menu.

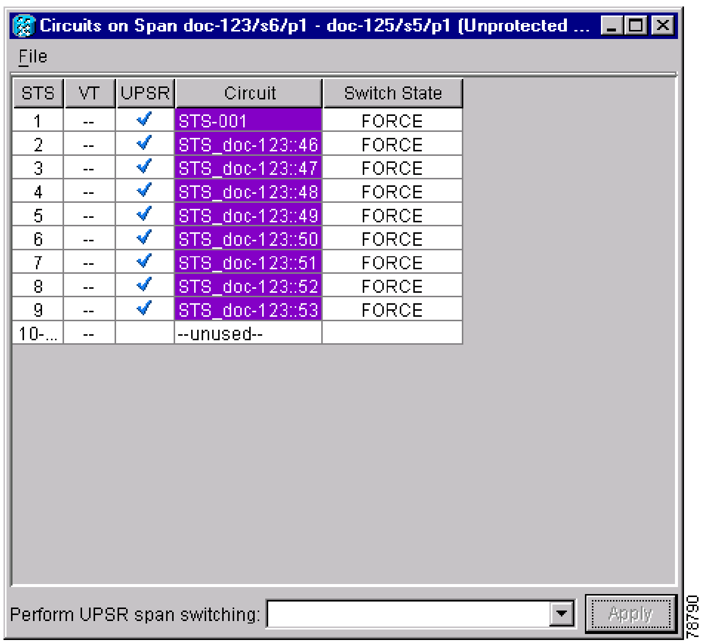
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all circuits is FORCE. Figure 16-5 shows an example.

Figure 16-5 Circuits on Span Dialog Box with a Force Switch



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.

Step 6 Return to your originating procedure (NTP).

DLP-A198 Clear a Path Protection Force Switch

Purpose	This task clears a path protection Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu at the node view, choose **Go to Network View**.

Step 2 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 3 In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.

Step 4 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 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.

Step 6 Return to your originating procedure (NTP).

NTP-A106 Remove a Path Protection Node

Purpose	This procedure removes a node from a path protection.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes, page 6-36
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals.

Caution If you remove a node that is the only BITS timing source for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that connect to other networks which are synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect customer service.

Step 1 Draw a diagram of the path protection where you will remove the node. In the diagram, identify the following:

- The node that is connected through its west port to the node that will be removed.
- The node that is connected through its east port to the node that will be removed.

Step 2 Log into a node in the network where you want to remove a path protection node. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that the path protection is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 9, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" procedure on page 11-18 for circuits that originate or terminate in the node you will remove. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.

Step 5 Complete the "DLP-A304 Verify Pass-Through Circuits" task on page 16-12 to verify that circuits passing through the target node enter and exit the node on the same STS and/or VT.

Step 6 Complete the "DLP-A197 Initiate a Path Protection Force Switch" task on page 16-16 for all spans connected to the node you are removing.

Step 7 Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 8 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Note If you delete a node that was in a login node group, you will see incomplete circuits for that node in CTC network view. (Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group.)

Step 9 Exit CTC and log back in. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions.

Step 10 Log into each newly connected node and click the **Alarms** tab. Verify that the span cards are free of alarms. Resolve any alarms before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 11 Complete the "DLP-A195 Verify Timing in a Reduced Ring" task on page 16-11.

Step 12 Complete the "DLP-A198 Clear a Path Protection Force Switch" task on page 16-18 to clear the protection switch.

Step 13 Click the **Circuits** tab and verify that no incomplete circuits are present.

Step 14 Complete the "NTP-A177 Path Protection Acceptance Test" procedure on page 6-38.

Stop. You have completed this procedure.

NTP-A262 Add a Node to a Linear ADM

Purpose	This procedure adds a single ONS 15454 node to the end of an ONS 15454 linear add/drop multiplexer (ADM) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 2-5 on page 2-31.

Note In a linear ADM configuration, two OC-N cards in 1+1 protection are connected to two OC-N cards in 1+1 protection on a second node. On the second node, two more OC-N cards are connected to a third node. The third node can be connected to a fourth node, and so on, depending on the number of nodes in the linear ADM. Slots 1 to 4 and 14 to 17 or Slots 5 to 6 and 12 to 13 can be used if connections between nodes are consistent. For example, Slot 5 on the first linear ADM node connects to Slot 5 on the second linear ADM node for the working path, and Slot 6 connects to Slot 6 for the protect path. The working OC-N ports have DCC terminations, and the OC-N cards are in a 1+1 protection group.

Caution If the linear ADM carries traffic, you cannot add a node between two linear nodes unless you delete and recreate the circuits. Use this procedure to add a node to the end of the linear ADM.

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for all the nodes in the ring.

Step 2 At the new node, complete one of the following procedures:

- If the node has not been turned up, complete all procedures in Chapter 4, "Turn Up Node."
- If the node has been turned up, complete the "NTP-A35 Verify Node Turn Up" procedure on page 6-2.

Step 3 Verify that the new node has two OC-N cards with the same rate as the linear ADM. If the OC-N cards are not installed, complete the "NTP-A16 Install the OC-N Cards" procedure on page 2-12.

Step 4 Complete "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 for the two OC-N cards that will connect to the linear ADM node.

Step 5 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for the working OC-N card at the new node. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination on the protect card.)

Note DCC failure alarms appear until you create DCC terminations in the linear ADM node and connect the fiber during Step 12.

Step 6 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the linear ADM node that will connect to the new node. If you are already logged in, continue with Step 7.

Step 7 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 8 Install the OC-N cards that will connect to the new node. See "NTP-A16 Install the OC-N Cards" procedure on page 2-12. If the cards are already installed, continue with Step 9.

Step 9 Connect the working card at the existing linear ADM node to the working card at the new node. See "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" procedure on page 2-33.

Step 10 Connect the protect card at the existing linear ADM node to the protect card at the new node.

Step 11 Complete "DLP-A73 Create a 1+1 Protection Group" task on page 4-30 for the two OC-N cards that connect to the new node.

Step 12 Complete the "DLP-A354 Provision SONET DCC Terminations" task on page 6-4 for the working OC-N card that connects to the working card on the new node. Make sure to set the Port State in the Create SDCC Termination dialog box to **IS**. (Do not create a DCC termination for the protect card.)

Step 13 From the View menu, choose **Go to Network View.** Verify that the newly created linear ADM configuration is correct. Two green span lines should appear between each linear node.

Step 14 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that no unexpected alarms or conditions are present.

Stop. You have completed this procedure.

NTP-A263 Remove a Node from a Linear ADM

Purpose	This procedure removes a single ONS 15454 from a linear ADM end node.
Tools/Equipment	None
Prerequisite Procedures	NTP-A38 Provision a Linear ADM Network, page 6-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution If the linear ADM carries traffic, you cannot remove a node between two linear nodes unless you delete and recreate the circuits. Use this procedure to remove a node to the end of the linear ADM.

Step 1 According to local site practice, complete the "NTP-A108 Back Up the Database" procedure on page 17-7 for all the nodes in the ring.

Step 2 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the linear ADM node that will be removed. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3.

Step 4 Click the **Circuits** tab. If the Scope field (lower-right corner) is not set to Node, change it to Node.

Step 5 If circuits originate or terminate on the node, complete the "DLP-A333 Delete Circuits and DWDM Optical Channel Network Connections" procedure on page 11-18 to remove them.

Step 6 Remove the DCC termination on the working OC-N linear ADM card. See "NTP-A255 Delete Communications Channel Terminations" task on page 12-20.

Step 7 Navigate to the node connected to the node that will be removed.

Step 8 Remove the DCC termination on the working OC-N linear ADM card that is connected to the node that will be removed. See the "NTP-A255 Delete Communications Channel Terminations" task on page 12-20.

Step 9 Remove the fiber from the OC-N cards connected to the node that will be removed.

Step 10 Display the network view to verify that the linear ADM configuration is correct. Two green span lines should appear between each linear node.

Step 11 Complete the "DLP-A298 Check the Network for Alarms and Conditions" task on page 15-3 to verify that no unexpected alarms or conditions are present.

Stop. You have completed this procedure.

Maintain the Node

This chapter provides procedures for maintaining the Cisco ONS 15454.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary. This section lists the chapter procedures (NTPs). Turn to a procedure to view its tasks (DLPs).

NTP-A107 Inspect and Maintain the Air Filter

Purpose	This procedure explains how to inspect and maintain reusable and disposable fan tray air filters.
Tools/Equipment	Spare air filters
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Note Although the filter can work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

Step 1 To maintain the reusable air filter, complete the "DLP-A199 Inspect, Clean, and Replace the Reusable Air Filter" task on page 17-2.

Step 2 To maintain the disposable air filter, complete the "DLP-A200 Inspect and Replace the Disposable Air Filter" task on page 17-5.

Stop. You have completed this procedure.

DLP-A199 Inspect, Clean, and Replace the Reusable Air Filter

Purpose	This task ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf.
Tools/Equipment	Vacuum or detergent and water faucet, spare filter, pinned hex key tool
Prerequisite Procedures	None
Required/As Needed	Inspection required every 30 days. Clean as needed.
Onsite/Remote	Onsite
Security Level	None

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.**

Step 1 Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.

Step 2 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that might have collected on the filter and proceed to Step 9. Figure 17-1 illustrates a reusable fan-tray air filter in an external filter bracket.

Step 3 If the filter is installed below the fan tray and not in the external filter brackets, open the front door of the shelf assembly. If the front door is already open, proceed to 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.

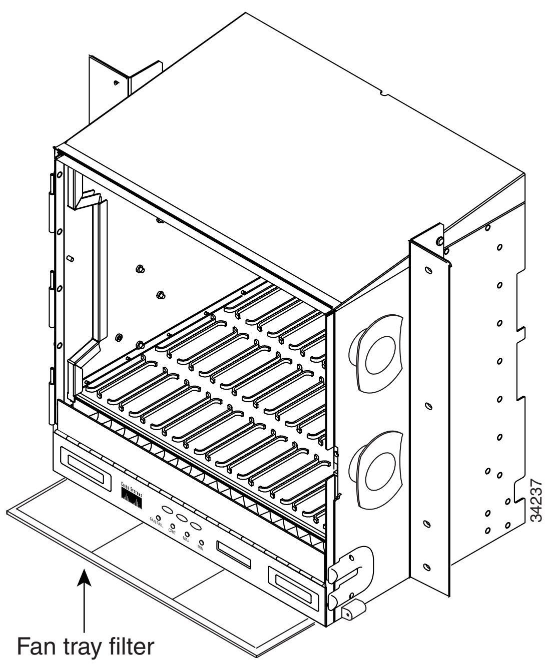
Step 4 Remove the front door (optional). If you do not want to remove the door or it is already removed, proceed to Step 5.

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.

Figure 17-1 Reusable Fan-Tray Air Filter in an External Filter Bracket (Front Door Removed)



Step 5 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 6 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 7 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 8 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.

Step 9 Visually inspect the air filter material for dirt and dust.

Step 10 If the reusable air filter contains a concentration of dirt and dust, replace the dirty air filter with a clean air filter (spare filters should be kept in stock) and reinsert the fan-tray assembly. Then, vacuum the dirty air filter or wash it under a faucet with a light detergent.

Caution Do not leave the fan tray out of the chassis for an extended period of time because excessive heat can damage the ONS 15454 cards.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 11 If you washed the filter, allow it to completely air dry for at least eight hours.

Warning **Do not put a damp filter back in the ONS 15454.**

Step 12 Replace the clean filter:

a. If the air filter is installed in the external filter brackets, slide the dry air filter all the way to the back of the brackets to complete the procedure.

b. If the filter is installed below the fan-tray assembly, remove the fan-tray assembly and slide the dry/clean 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 13 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 14 Rotate the retractable handles back into their compartments.

Step 15 If you replace the door, also reattach the ground strap.

Step 16 Close and lock the door.

Step 17 Return to your originating procedure (NTP).

DLP-A200 Inspect and Replace the Disposable Air Filter

Purpose	This task ensures that the air filter is free from dirt and dust, thus allowing optimum air flow and preventing dirt and dust from entering the ONS 15454.
Tools/Equipment	Extra filters, pinned hex key
Prerequisite Procedures	None
Required/As Needed	Inspection required every 30 days. Replace as needed.
Onsite/Remote	Onsite
Security Level	None

Note The disposable air filter is installed below 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 front door is already open, proceed to 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 the door is already removed or you do not want to remove it, proceed to Step 4.

a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

c. Secure the dangling end of the ground strap to the door or chassis with tape.

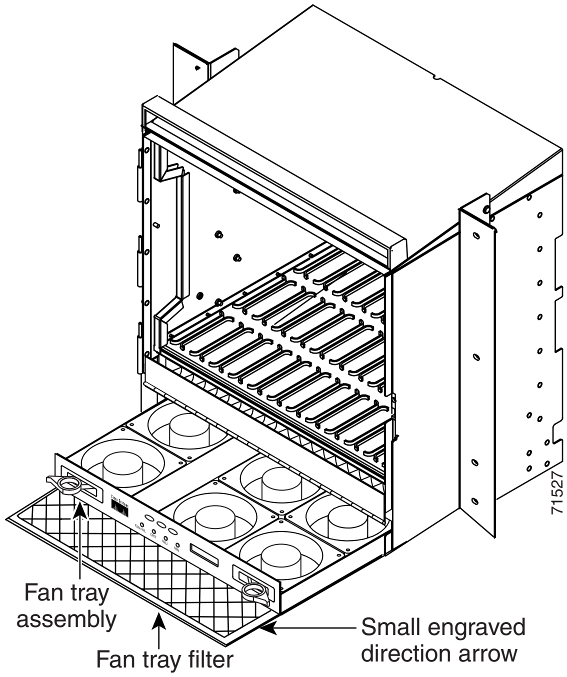
Step 4 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 17-2).

Caution Do not leave the fan tray out of the chassis for an extended period of time because excessive heat can damage the ONS 15454 cards.

Figure 17-2 Inserting or Removing the Fan-Tray Assembly (Front Door Removed)

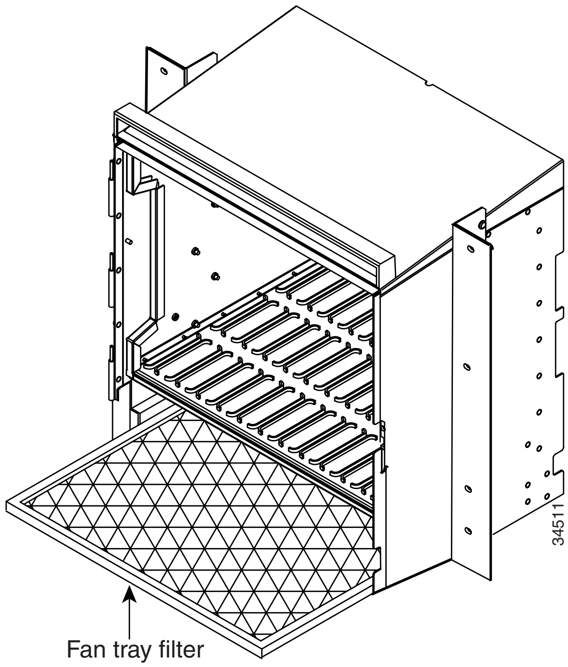


Step 7 Gently remove the air filter from the shelf assembly (Figure 17-3). Be careful not to dislodge any dust that might have collected on the filter.

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 new 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 17-3 Inserting or Removing a Disposable Fan-Tray Air Filter (Front Door Removed)



Step 10 Slide the fan-tray assembly into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 11 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 12 Rotate the retractable handles back into their compartments.

Step 13 If you replace the door, also reattach the ground strap.

Step 14 Close and lock the door.

Step 15 Return to your originating procedure (NTP).

NTP-A108 Back Up the Database

Purpose	This procedure stores a backup version of the TCC2 (software) database on the workstation running Cisco Transport Controller (CTC) or on a network server.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
Onsite/Remote	Onsite or remote
Security Level	Maintenance

Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

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

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node you want to back up. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Database** tabs.

Step 3 Click **Backup**.

Step 4 Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the .db file extension; for example, database.db.

Step 5 Click **Save**.

Step 6 Click **OK** in the confirmation dialog box.

Stop. You have completed this procedure.

NTP-A109 Restore the Database

Purpose	This procedure restores the TCC2 software database.
Tools/Equipment	None
Prerequisite Procedures	NTP-A108 Back Up the Database, page 17-7
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Note For information on restoring the ML-Series card, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.

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 approximately one minute after the TCC2 reboot has completed on each node before proceeding to the next node.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you are restoring the database. If you are already logged in, continue with Step 2.

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

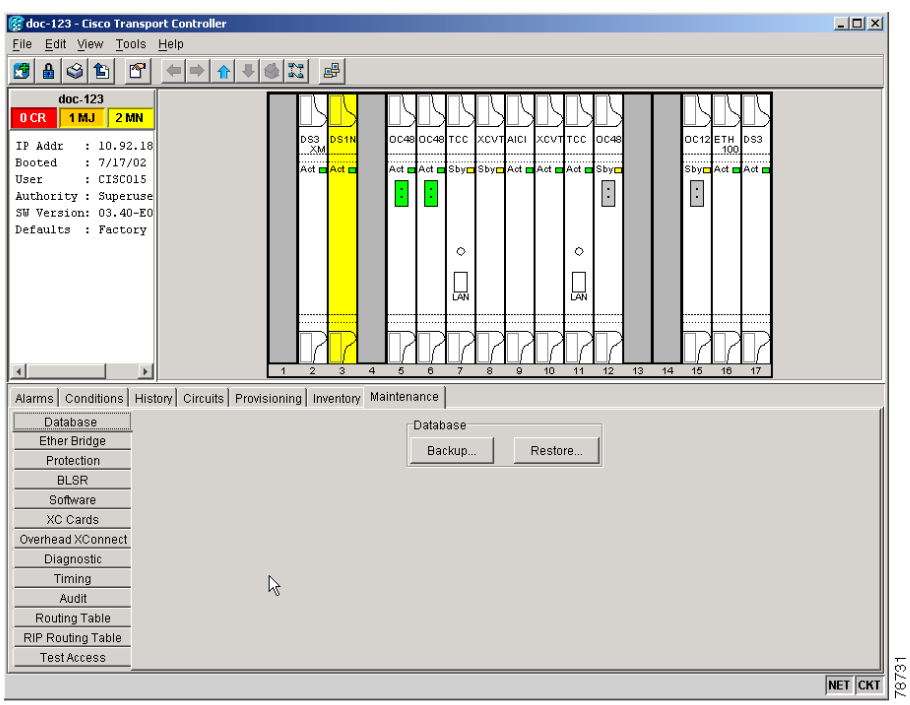
Step 3 If switch events need to be cleared, in node view click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

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

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

Step 4 In node view, click the **Maintenance > Database** tabs (Figure 17-4).

Figure 17-4 Restoring the TCC2 Database



Step 5 Click **Restore**.

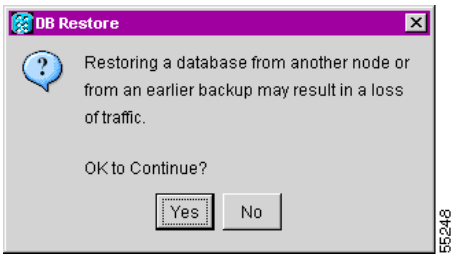
Step 6 Locate the database file stored on the workstation hard drive or on network storage.

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

Step 7 Click the database file to highlight it.

Step 8 Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup may affect traffic on the login node (Figure 17-5).

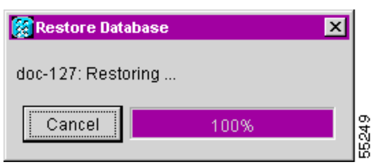
Figure 17-5 Restoring the Database—Traffic Loss Warning



Step 9 Click **Yes**.

The Restore Database dialog box monitors the file transfer (Figure 17-6).

Figure 17-6 Restoring the Database – In-Process Notification



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

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

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

Stop. You have completed this procedure.

NTP-A163 Restore the Node to Factory Configuration

Purpose	This procedure clears the TCC2 database and restores customer or factory defaults by uploading the most recent software package and a blank database. This process is performed using the RE-INIT.jar utility, also called the reinitialization (reinit) tool.
Tools/Equipment	Software CD containing Software Release 3.4 or later, the node NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer you use to perform this procedure.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 17-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

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 may accidentally copy an incorrect database if multiple databases are kept in the specified directory.

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

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

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

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

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

Step 1 If you need to install or replace one or more TCC2 cards, see the "DLP-A36 Install the TCC2 Cards" task on page 2-7.

Step 2 If you are using Microsoft Windows, complete the "DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 17-12.

Step 3 If you are using UNIX, complete the "DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 17-14.

Stop. You have completed this procedure.

DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This procedure describes how to use the reinitialization tool in Windows. Use this tool to clear the database on the TCC2, upload software, and restore factory or customer defaults.
Tools/Equipment	Software CD containing Software R3.4 or later, the NE defaults, and the reinitialization tool Straight-through (CAT-5) LAN cable JRE 1.03_02 must be installed on your PC
Prerequisite Procedures	NTP-A108 Back Up the Database, page 17-7
Required/As Needed	As needed to clear the existing database from a TCC2 and restore the node default settings.
Onsite/Remote	Onsite
Security Level	Superuser

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

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

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

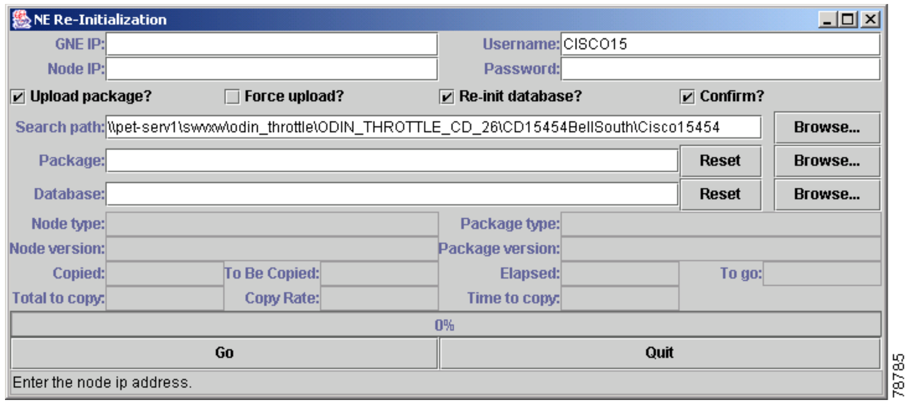
Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard opens, click **Cancel**.

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 choose **All Files from the Files of Type** drop-down menu.

Step 4 Select the RE-INIT.jar file and click **Open** to open the reinit tool (Figure 17-7).

Figure 17-7 Reinitialization Tool in Windows



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

Step 6 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 17-7).

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

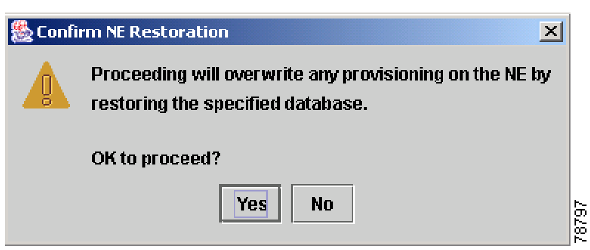
Step 8 Verify that the Re-Init Database, Upload Package, and Confirm checkboxes are checked. If one is not checked, check the checkbox.

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

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

Step 10 Click **Go**. A confirmation dialog box opens (Figure 17-8).

Figure 17-8 Confirming NE Restoration



Step 11 Click **Yes**.

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

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

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

Step 14 Manually set the node name and network configuration to site-specific values. See the "NTP-A25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-7 and "NTP-A169 Set Up CTC Network Access" procedure on page 4-9 for information on setting the node name, IP address, subnet mask and gateway, and IIOP port.

Step 15 Return to your originating procedure (NTP).

DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task describes how to use the reinitialization tool in a UNIX environment. Use this tool to clear the database on the TCC2 card and restore factory or customer defaults.
Tools/Equipment	Software CD containing Software R3.4 or later, the node NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer that you use to perform this procedure.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 17-7
Required/As Needed	As needed to clear the existing database from a TCC2 card and restore the node default settings.
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

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

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

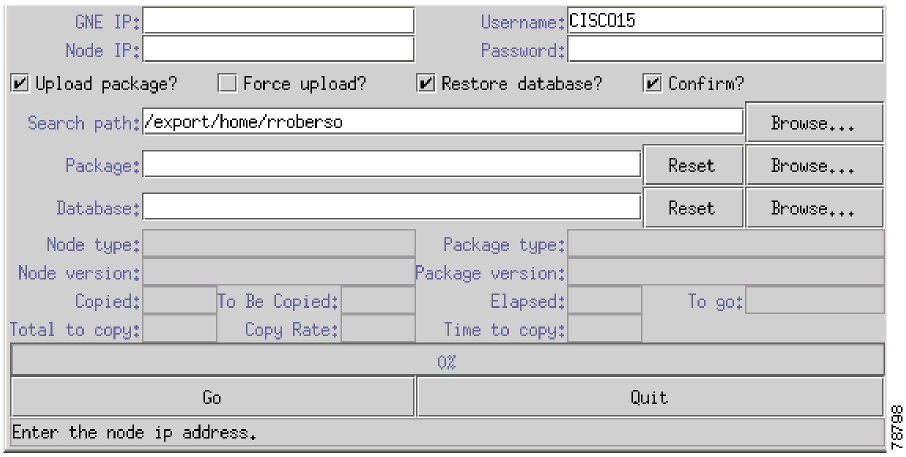
Note JRE 1.03_02 must also be installed on the computer you use to perform this procedure.

Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard 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 17-9). If you are working with a command line interface, run **java -jar RE-INIT.jar**.

Figure 17-9 The Reinitialization Tool in UNIX



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

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 17-9).

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

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

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

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

Step 9 Click **Go**. A confirmation dialog box opens (Figure 17-8 on page 17-13).

Step 10 Click **Yes**.

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

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

Step 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 TCC2 card or on the hub or switch where the ONS 15454 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC.

Step 13 Set the node name and network configuration to site-specific values. See the "NTP-A81 Change Node Management Information" procedure on page 12-2 and the "NTP-A201 Change CTC Network Access" procedure on page 12-4 for information on provisioning the node name, IP address, subnet mask and gateway, and IIOP port.

Step 14 Return to your originating procedure (NTP).

NTP-A214 Off-Load the Security Audit Trail Log

Purpose	This procedure stores up to 640 audit trail log entries in a local or network drive file to maintain a record of actions performed for the node. If the audit trail log is not off-loaded, the oldest entries are overwritten after the log reaches capacity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to off-load the audit trail log. If you are already logged in, continue with Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

Step 4 Click **Archive**.

Step 5 In the Archive Audit Trail dialog, navigate to the directory (local or network) where you want to save the file.

Step 6 Enter a name in the File Name field.

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

Step 7 Click **Save**.

The 640 entries are saved in this file. The next entries continue with the next number in the sequence, rather than starting over.

> **Note** Archiving does not delete entries from the CTC audit trail log. However, entries can be self-deleted by the system after the log maximum is reached. If you archived the entries, you cannot reimport the log file back into CTC and will have to view the log in a different application.

Stop. You have completed this procedure.

NTP-A110 Inhibit Card Protection Switching

Purpose	This procedure describes how to apply and remove a Lock On or Lock Out to a traffic card in a linear protection configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-A170 Create Protection Groups, page 4-26
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to apply a Lock On or Lock Out. If you are already logged in, continue with Step 2.

Step 2 To prevent traffic on a working or protect card from switching to the other card in the pair, complete the "DLP-A201 Apply a Lock On" task on page 17-17.

Step 3 To prevent traffic from switching to the protect card, complete the "DLP-A202 Apply a Lock Out" task on page 17-18.

Note A combination of Lock On and Lock Out is allowed in 1:1 and 1:N protection; for example, a Lock On on the working card and a Lock Out on the protect card is permissible.

Step 4 To remove a Lock On or Lock Out and return a protection group to its usual switching method, complete the "DLP-A203 Clear a Lock On or Lock Out" task on page 17-19.

Note A non-alarmed event (INHSW) is raised when a card is placed in a Lock On or Lock Out state.

Stop. You have completed this procedure.

DLP-A201 Apply a Lock On

Purpose	This task prevents traffic from being switched from one card to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note To apply a Lock On to a protect card in a 1:1 or 1:N protection group, the protect card must be active. If the protect card is in standby, the Lock On button is disabled. To make the protect card active, you must switch traffic from the working card to the protect card (Step 4). When the protect card is active, you can apply the Lock On.

Step 1 Use the following rules to determine if you can apply a Lock On:

- For a 1:1 electrical protection group, the working or protect cards can be placed in the Lock On state.
- For a 1:N electrical protection group, the working or protect cards can be placed in the Lock On state.
- For a 1+1 optical protection group, only the working port can be placed in the Lock On state.
- For a Y-cable protection group, only the working port can be placed in the Lock On state.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 In the Protection Groups list, click the protection group where you want to apply a Lock On.

Step 4 If you determine that the protect card is in standby mode and you want to apply the Lock On to the protect card, make the protect card active:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

Step 5 In the Selected Group list, click the active card where you want to lock traffic.

Step 6 In the Inhibit Switching area, click **Lock On**.

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

The Lock On has been applied and traffic cannot be switched to the working card. To clear the Lock On, see the "DLP-A203 Clear a Lock On or Lock Out" task on page 17-19.

Step 8 Return to your originating procedure (NTP).

DLP-A202 Apply a Lock Out

Purpose	This task switches traffic from one card to another using a Lock Out, which is a switching mechanism that overrides other external switching commands (Force, Manual, and Exercise).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note Multiple Lock Outs in the same protection group are not allowed.

Step 1 Use the following rules to determine if you can put the intended card in a Lock Out state:

- For a 1:1 electrical protection group, you can apply a Lock Out to the working or protect cards.
- For a 1:N electrical protection group, you can apply a Lock Out to the working or protect cards.
- For a 1+1 optical protection group, you can apply a Lock Out to the protect port.
- For a Y-cable protection group, you can apply a Lock Out to the protect port.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 In the Protection Groups list, click the protection group that contains the card you want to Lock Out.

Step 4 In the Selected Group list, click the card you want to lock traffic out of.

Step 5 In the Inhibit Switching area, click **Lock Out**.

Step 6 Click **Yes** in the confirmation dialog box.

The Lock Out has been applied and traffic is switched to the opposite card. To clear the Lock Out, see the "DLP-A203 Clear a Lock On or Lock Out" task on page 17-19.

Note Provisioning a Lock Out raises a LOCKOUT-REQ or an FE-LOCKOUT-PR condition in CTC. Clearing the Lock Out switch request clears these conditions.

Step 7 Return to your originating procedure (NTP).

DLP-A203 Clear a Lock On or Lock Out

Purpose	This task clears a Lock On or Lock Out.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
	DLP-A201 Apply a Lock On, page 17-17 or
	DLP-A202 Apply a Lock Out, page 17-18
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

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

The Lock On or Lock Out is cleared.

Step 6 Return to your originating procedure (NTP).

NTP-A111 Revert to an Earlier Software Load

Purpose	This procedure reverts the ONS 15454 database to an earlier software load.
Tools/Equipment	None

Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	As needed
Onsite/Remote	On site or remote
Security Level	Superuser

Tip The revert feature is useful if a maintenance window closes while you are upgrading CTC software. You can revert to the protect software load without losing traffic. When the next maintenance window appears, complete the upgrade and activate the new software load.

Caution Provisioning performed after a software load is activated (upgraded to a higher software release) will not reinstate with a revert. The database configuration at the time of activation is reinstated by a revert.

Note Reverting to a 2.2.1 or later load switches to the older software load and its database without affecting traffic or DCC connectivity. This feature requires dual TCC2 cards and CTC Software R 2.2.1 or later as the protect version.

Note Circuits created and provisioning performed after a software load is activated (upgraded to a later software release) do not reinstate with a revert. The database configuration at the time of activation is reinstated after a revert. This note does not apply to maintenance reverts (for example, R2.2.2 to R2.2.1), because maintenance releases use the same database.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 to log into the node you want to revert. If you are already logged in, continue with Step 2.

Step 2 Record the IP address of that node; the IP address is displayed on the left side of the node view window.

> **Note** To find the IP address you can also click the **Provisioning > Network > General** tabs.

Step 3 If you are reverting to a previous software release (not a maintenance release), record any new circuits created since the previous software upgrade because these circuits have to be manually recreated after the software reversion if you still need to have them.

Step 4 Click the **Maintenance > Software** tabs.

Step 5 Verify that the protect software is Software R2.2.0 or later. If the protect software is not Software R2.2.0 or later, do not revert.

> **Note** The TCC2 card is compatible with Software R4.0 and later.

Step 6 Click **Revert**. The Revert button activates the protect software load.

Step 7 Click **Yes** in the revert confirmation dialog box. The ONS 15454 reboots and loses the connection to CTC.

Step 8 Wait until the software upgrade finishes. This might take as long as 30 minutes.

Step 9 When the software upgrade is finished, click the **Delete CTC Cache** button in the browser window.

Step 10 Completely close the browser.

Step 11 Restart the browser and log back into the node using the IP address recorded in Step 2.

The browser downloads the CTC applet for the protect software load.

Step 12 If needed, recreate the circuits recorded in Step 3. See Chapter 8, "Create Circuits and VT Tunnels" for specific circuit creation procedures.

Stop. You have completed this procedure.

NTP-A112 Clean Fiber Connectors

Purpose	This procedure cleans the fiber connectors.
Tools/Equipment	Inspection microscope Compressed air/duster "Type A" Fiber Optic Connector Cleaner (CLETOP reel) Isopropyl alcohol 70% or higher Optical swab Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Note Replace all dust caps whenever the equipment is unused for 30 minutes or more.

Step 3 Complete the "DLP-A204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes" task on page 17-22 as necessary.

Step 4 Complete the "DLP-A205 Clean Fiber Connectors with CLETOP" task on page 17-22 as necessary.

Step 5 Complete the "DLP-A206 Clean the Fiber Adapters" task on page 17-23 as necessary.

Caution Do not reuse optical swabs. Keep unused swabs off of work surfaces.

Stop. You have completed this procedure.

DLP-A204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes

Purpose	This task cleans the fiber connectors and adapters with alcohol and dry wipes.
Tools/Equipment	Compressed air/duster Isopropyl alcohol 70% or higher Optical swab Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

Step 1 Remove the dust cap from the fiber connector.

Step 2 Wipe the connector tip with the premoistened alcohol wipe.

Step 3 Blow-dry using filtered air.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 to 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-A205 Clean Fiber Connectors with CLETOP

Purpose	This task cleans the fiber connectors with CLETOP.
Tools/Equipment	"Type A" Fiber Optic Connector Cleaner (CLETOP reel) Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the dust cap from the fiber connector.

Step 2 Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

Step 3 Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 to 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

> **Note** If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-A206 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	CLETOP stick swab
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.

Step 3 Place dust plugs on the fiber adapters when not in use.

Step 4 Return to your originating procedure (NTP).

NTP-A113 Reset the TCC2 Card Using CTC

Purpose	This procedure resets the TCC2 card and switches the node to the redundant card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2 Cards, page 2-7
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Note Before you reset the TCC2, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note When a software reset is performed on an active TCC2, the AIC or AIC-I card goes through an initialization process and also resets. The AIC or AIC-I card reset is normal and happens each time an active TCC2 card goes through a software-initiated reset.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to reset the TCC2 card. If you are already logged in, continue with Step 2.

Step 2 In node view, right-click the TCC2 card to reveal a shortcut menu.

Step 3 Click **Reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note For LED behavior during a TCC2 reboot, see Table 4-1 on page 4-12.

Step 6 Confirm that the TCC2 card LED is amber (standby).

Stop. You have completed this procedure.

NTP-A215 View G-Series Ethernet Maintenance Information

Purpose	This procedure enables you to view loopback, bandwidth, and J1 path trace information for G-Series Ethernet cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A246 Install Ethernet Cards and Connectors, page 2-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click a G-Series Ethernet card. The card view appears.

Step 3 To view loopback status, click the **Maintenance > Loopback** tabs.

The Port and State columns identify the port number and current circuit state (IS, OOS, OOS_MT) for each port. The Loopback Type column identifies the type of loopback [None, Terminal (Inward), or Facility {Line)] applied to each port on the card.

Step 4 To view Ethernet bandwidth utilization, click the **Maintenance > Bandwidth** tabs.

Step 5 Click **Retrieve Bandwidth Usage**.

The current STS bandwidth usage information appears.

Step 6 To view J1 path trace information, click the **Maintenance > J1 Path Trace** tabs and then **click Retrieve**.

Stop. You have completed this procedure.

NTP-A239 View E-Series Ethernet Maintenance Information

Purpose	This procedure enables you to view maintenance information for E-Series Ethernet cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-A246 Install Ethernet Cards and Connectors, page 2-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note The E-Series Maintenance tab is not implemented in this release.

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24. If you are already logged in, continue with Step 2.

Step 2 To view spanning tree information, in node view click the **Maintenance > Ether Bridge > Spanning Trees** tabs.

Step 3 As needed, complete the following tasks:

- DLP-A309 View the Ethernet MAC Address Table, page 17-26
- DLP-A310 View Ethernet Trunk Utilization, page 17-26

Stop. You have completed this procedure.

DLP-A309 View the Ethernet MAC Address Table

Purpose	This task displays the Ethernet MAC address table for any node with one or more E-Series Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > MAC Table** tabs.

Step 2 Select the appropriate E-Series Ethernet card in the Layer 2 Domain field.

Step 3 Click **Retrieve**.

The MAC address table information is displayed.

Step 4 Return to your originating procedure (NTP).

DLP-A310 View Ethernet Trunk Utilization

Purpose	This task displays the Ethernet Trunk bandwidth usage on any node with one or more E-Series Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > Trunk Utilization** tabs.

Step 2 Select the desired time interval in the Interval field.

Step 3 Click **Refresh**.

The trunk utilization information for the current and previous time intervals is displayed.

Step 4 Return to your originating procedure (NTP).

NTP-A218 Change the Node Timing Reference

Purpose	This procedure enables automatic timing reference switching or returns the node timing to normal operation.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to enable timing switching. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-A322 Manual or Force Switch the Node Timing Reference" task on page 17-27 as needed.

Step 3 Complete the "DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference" task on page 17-28 as needed.

Stop. You have completed this procedure.

DLP-A322 Manual or Force Switch the Node Timing Reference

Purpose	This task commands the node to switch to the timing reference you have selected if the synchronization status message (SSM) quality of the requested reference is not less than the current reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs.

Step 2 From the Reference drop-down list for the desired Clock, choose the desired reference.

Step 3 From the Operation drop-down list for the desired Clock, choose one of the following options:

- **Manual**—This operation commands the node to switch to the reference you have selected if the SSM quality of the reference is not lower than the current timing reference.
- **Force**—This operation commands the node to switch to the reference you have selected, regardless of the SSM quality (if the reference is valid).

For information about the Clear option, see the "DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference" task on page 17-28.

Step 4 Click **Apply** next to the timing source.

Step 5 Click **Yes** in the confirmation dialog box. If the selected timing reference is an acceptable valid reference, the node switches to the selected timing reference.

Step 6 If the selected timing reference is invalid, a warning dialog appears. Click **OK**; the node does not revert to the normal timing reference.

Step 7 Return to your originating procedure (NTP).

DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference

Purpose	This task clears a Manual or Force switch on a node timing reference and reverts the timing reference to its provisioned reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs.

Step 2 Find the Clock reference that is currently set to Manual or Force in the Operation menu.

Step 3 From the Operation pull-down menu choose **Clear**.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box. If the normal timing reference is an acceptable valid reference, the node switches back to the normal timing reference as defined by the system configuration.

Step 6 If the normal timing reference is invalid or has failed, a warning dialog appears. Click **OK**; the timing reference does not revert.

Step 7 Return to your originating procedure (NTP).

NTP-A223 View the ONS 15454 Timing Report

Purpose	This procedure displays the current status of the ONS 15454 timing references.
Tools/Equipment	None
Prerequisite Procedures	NTP-A28 Set Up Timing, page 4-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-A60 Log into CTC" task on page 3-24 at the node where you want to view the node timing status. If you are already logged in, continue with Step 2.

Step 2 Click the **Maintenance > Timing > Report** tabs.

Step 3 In the Timing Report area, you can view node timing information. The date and time of the report appear at the top of the report. The time stamp is the same as the alarms time stamp and can be configured using the "DLP-A112 Display Alarms and Conditions Using Time Zone" task on page 9-10. Table 17-1 on page 17-29 describes the report fields and entries.

Step 4 To update the report, click **Refresh**.

Table 17-1 ONS 15454 Timing Report

Item	Description	Option	Option Description
Clock	Indicates the timing clock. The report section that follows applies to the timing clock indicated.	NE	The node timing clock.
		BITS-1 Out	The BITS-1 Out timing clock.
		BITS-2 Out	The BITS-2 Out timing clock.

Table 17-1 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Status	Indicates the status of the timing clock.	INIT_STATE	The timing reference has not been provisioned. For an NE reference, this status appears just before the first provisioning messages when the TCC2 is booting. Timing is provisioned to the internal clock of the node.
		HOLDOVER_STATE	The clock was locked onto a valid timing reference for more than 140 seconds when a failure occurred. Holdover state timing is a computation based on timing during normal state combined with the node's internal clock. The node holds onto this frequency until the valid reference is restored. This status appears for NE references only.
		FREERUN_STATE	The node is running off its internal clock without any modification except the calibrated value to bring timing to 0 PPM. Freerun state can occur when a Force switch to the Internal clock is initiated, all references fail without the 140 seconds of holdover data, or only Internal timing references are defined. This status appears for NE references only.
		NO_SYNC_STATE	A synchronization timing reference is not defined. BITS-1 Out or BITS-2 Out default to this status until an OC-N card is defined as its reference on the Provisioning > Timing tab. This status appears for external references only.
		NE_SYNCH_STATE	BITS-1 Out and BITS-2 Out use the same timing source as the NE. This is displayed when NE Reference is selected for BITS-1 Out and BITS-2 Out Reference List on the Provisioning > Timing tab.
		NORMAL_STATE	The timing reference is locked onto one of its provisioned references. The reference cannot be Internal or no sync state.
		FAST_START_STATE	The node has switched references, but the reference is too far away to reach normal state within an acceptable amount of time. Fast Start is a fast acquisition mode to allow the node to quickly acquire the reference. After it achieves this goal, the node progresses to the normal state.
		FAST_START_FAILED_STATE	A timing reference is too far away to reach in normal state. The fast start state could not acquire sufficient timing information within the allowable amount of time.
Status Changed At	Date and time of the last status change.	—	—
Switch Type	Type of switch.	AUTOMATIC	The timing switch was system-generated.
		Manual	The timing switch was a user-initiated Manual switch.
		Force	The timing switch was user-initiated Force switch.

Table 17-1 ONS 15454 Timing Report (continued)

Item	Description	Option	Option Description
Reference	Indicates the timing reference.	Three timing references are available on the Provisioning > Timing tab.	—
Selected	Indicates whether the reference is selected.	Selected references are indicated with an X.	—
Facility	Indicates the timing facility provisioned for the reference on the Provisioning > Timing tab.	BITS-1	The timing facility is a BITS clock attached to the node's BITS-1 pins.
		BITS-2	The timing facility is a BITS clock attached to the node's BITS-2 pins.
		OC-N card with port #	If the node is set to line timing, the OC-N card and port provisioned as the timing reference.
		Internal clock	The node is using its internal clock.
State	Indicates the timing reference state.	IS	The timing reference is in service.
		OOS	The timing reference is out of service.
Condition	Indicates the timing reference state.	OKAY	The reference is valid to use as a timing reference.
		OOB	Out of bounds; the reference is not valid and cannot be used as a timing reference, for example, a BITS clock is disconnected.
Condition Changed	Indicates the date and time of the last status change in MM/DD/YY HH:MM:SS format.	—	—
SSM	Indicates whether SSM is enabled for the timing reference.	Enabled	SSM is enabled.
		Disabled	SSM is not enabled.
SSM Quality	Indicates the SSM timing quality.	8 to 10 SSM quality messages might be displayed.	For a list of SSM message sets, see the "Security and Timing" chapter in the *Cisco ONS 15454 Reference Manual*.
SSM Changed	Indicates the date and time of the last SSM status change in MM/DD/YY HH:MM:SS format.	—	—

Stop. You have completed this procedure.

CHAPTER 18

Power Down the Node

This chapter explains how to power down a node and stop all node activity on the Cisco ONS 15454.

Note Except where noted, this procedure applies to both multiservice transport protocol (MSTP) and SONET platform nodes.

NTP-A114 Power Down the Node

Purpose	This procedure stops all node activity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	For software steps the provisioning level or higher is required. For hardware steps any level is allowed.

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 The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.

Note Always use the supplied ESD wristband when working with the Cisco ONS 15454. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf on the NEBS 3 shelf assembly. To access the ESD plug on the NEBS 3 shelf assembly, open the front door of the Cisco ONS 15454. The front door is grounded to prevent electrical shock.

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 16. If cards are installed, log into the node. See the "DLP-A60 Log into CTC" task on page 3-24 for instructions.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Verify that the node is not connected to a network.

a. If the node is part of a working network, log out of the node and complete the "NTP-A263 Remove a Node from a Linear ADM" procedure on page 16-21, the "NTP-A213 Remove a BLSR Node" procedure on page 16-9, or the "NTP-A106 Remove a Path Protection Node" procedure on page 16-18. If the node is part of a Software R4.6 MSTP configuration, consult your network administrator. Continue with Step 4.

b. If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 4.

Note Current configurations will be saved if Steps 4–16 are skipped.

Step 4 In node view, click the **Circuits** tab and verify that no circuits are displayed, then proceed to Step 5. If circuits are displayed, delete all the circuits that originate or terminate in the node, as follows:

a. Click the circuits that need to be deleted and click **Delete**.

b. Click **Yes**.

Repeat until no circuits are displayed.

Step 5 In node view, click the **Provisioning > Protection** tabs and delete all protection groups:

a. Click the protection group that needs to be deleted and click **Delete**.

b. Click **Yes**.

Repeat until no protection groups are displayed.

Step 6 In node view, click the **Provisioning > DCC/GCC/OSC** tabs and delete all SDCC or OSC terminations:

a. Click the SDCC or OSC termination that needs to be deleted and click **Delete**.

b. Click **Yes**.

Repeat until no SDCC or OSC terminations are present.

Step 7 For each installed OC-N or DS-N card, place all ports in Out of Service status:

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

b. Click under the Status column for each port and choose **Out of Service**.

Step 8 For each installed MSTP channel-bearing card, place all lines and channels in Out of Service status:

a. In the card view, click the **Provisioning > Optical Line > Parameters** tabs.

b. Click under the Status column for each line and choose **Out of Service**.

c. Click the **Provisioning > Optical Chn > Parameters** tabs.

d. Click under the Status column for each channel and choose **Out of Service**.

Step 9 For each installed MSTP band-bearing card, place all lines and bands in Out of Service status:

a. In the card view, click the **Provisioning > Optical Line > Parameters** tabs.

b. Click under the Status column for each line and choose **Out of Service**.

c. Click the **Provisioning > Optical Band > Parameters** tabs.

d. Click under the Status column for each band and choose **Out of Service**.

Step 10 For each installed DWDM transponder (TXP) or Muxponder (MXP) card, place all lines in Out of Service status:

a. In the card view, click the **Provisioning > Line > SONET** tabs if the card was provisioned for a SONET payload, or the **Provisioning > Line > SDH** tabs if the card was provisioned for an SDH payload.

b. Click under the Status column for each line and choose **Out of Service**.

Step 11 Remove all fiber connections to the cards.

Step 12 In node view, right-click an installed card and click **Delete**.

Step 13 Click **Yes**.

Step 14 After you have deleted the card, open the card ejectors and remove it from the node.

Step 15 Repeat Step 7 through 14 for each installed card.

Note You cannot delete a TCC2 card in CTC. Physically remove it after all the other cards have been deleted and removed.

Step 16 Shut off the power from the power supply that feeds the node.

Step 17 Disconnect the node from its external fuse source.

Step 18 Store all the cards you removed and update inventory records according to local site practice.

Stop. You have completed this procedure.

CTC Information and Shortcuts

This appendix describes the Cisco Transport Controller (CTC) views, menus and tool options, shortcuts, and table display options. This appendix also describes the shelf inventory data presented in CTC. For more information about CTC, refer to the *Cisco ONS 15454 Reference Manual*.

Display Node, Card, and Network Views

CTC provides three views of the ONS 15454 and ONS network:

- Node view appears when you first log into an ONS 15454. This view shows a graphic of the ONS 15454 shelf and provides access to tabs and subtabs that you use to manage the node.
- Card view provides access to individual ONS 15454 cards. This view provides a graphic of the card and provides access to tabs and subtabs that you use to manage the card.
- Network view shows all the nodes in a ring. A Superuser can set up this feature so each user will see the same network view, or the user can create a custom view with maps. This view provides access to tabs and subtabs that you use to manage the network.

Table A-1 lists different actions for changing CTC views.

Table A-1 Change CTC Views

To display:	Perform one of the following:
Node view	• Log into a node; node view is the default view. • In network view, double-click a node icon, or right-click the node and choose **Open Node** from the shortcut menu. • In network view, single-click a node icon, then choose **Go To Selected Object View** from the View menu. • From the View menu, choose **Go To Other Node**, then choose the node you want from the shortcut menu. • Use the arrows on the CTC toolbar to navigate up or down views. For example, in network view, click a node, then click the down arrow.

Table A-1 Change CTC Views (continued)

To display:	Perform one of the following:
Network view	• In node view, click the up arrow or the Network View tool on the CTC toolbar. • From the View menu, choose **Go To Network View**.
Card view	• In node view, double-click a card or right-click the card and choose **Open Card**. • In node view, single-click a card icon, then choose **Go To Selected Object View** from the View menu. • Use the arrows on the CTC toolbar to navigate up or down views. For example, in node view, click a card, then click the down arrow.

Node Icons on the Network View Map

Table A-2 lists the node icons on the network view map.

Table A-2 Description of Node Icons on Network View Map

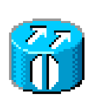
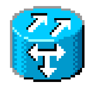
Node Name	Icon	Description
SONET Hybrid OADM Hybrid line amplifier Hybrid terminal Passive hybrid terminal Amplified TDM		A SONET, hybrid, or amplified TDM node icon are represented as a cylinder with crossed arrows. • A SONET node can include OC-N cards, electrical cards, cross-connects, and more. • A hybrid optical add/drop multiplexer (OADM) contains at least one AD-xC or one AD-xB and two TCC2 cards. TDM cards can be installed in any available slot. • A hybrid line amplifier contains amplifiers and both TDM and dense wavelength division multiplexing (DWDM) cards. • A hybrid terminal node contains at least one 32 MUX-O card, one DMX-O card, amplifiers, two TCC2 cards, and TDM cards. • A passive hybrid terminal node has the same equipment as the hybrid terminal node, but does not contain amplifiers. • An amplified TDM node is a node that increases the span length between two ONS 15454 nodes that contain TDM cards and optical amplifiers. Amplified TDM nodes contain either OPT-BST amplifiers or AD-1C cards.
Hub		A DWDM hub node icon is represented as a three-dimensional cylinder with amplifiers. A hub node contains at least two 32-channel demultiplexers and two 32-channel multiplexers. No OADM cards are provisioned.

Table A-2 Description of Node Icons on Network View Map (continued)

Node Name	Icon	Description
OADM		A DWDM OADM node icon is represented as a three-dimensional cylinder with arrows. An OADM node contains at least one AD-xC or AD-xB. No 32-channel multiplexer and 32-channel demultiplexer cards are provisioned.
Terminal (west)		These nodes are represented as a three-dimensional cylinder with one amplifier on the west side of the icon. • A terminal node contains one 32-channel demultiplexer and one 32-channel multiplexer. No OADM cards are provisioned. • A flexible terminal node contains a series of OADM and amplifier cards.
Terminal (east)		These nodes are represented as a three-dimensional square with one amplifier on the east side of the icon. • A terminal node contains one 32-channel demultiplexer and one 32-channel multiplexer. No OADM cards are provisioned. • A flexible terminal node contains a series of OADM and amplifier cards.
Line OSC regeneration line		These nodes are represented as a three-dimensional cylinder with one arrow pointing west and another arrow pointing east. • A line node only has OPT-PRE or OPT-BST amplifiers provisioned. • An optical service channel (OSC) regeneration line node contains two OSC-CSM cards.
Unknown		An unknown DWDM node icon is represented as a three-dimensional cylinder with one arrow pointing north. An unknown node means that the provisioned cards do not allow the node to fit in with any of the defined DWDM node categories.

Manage the CTC Window

Different navigational methods are available within the CTC window to access views and perform management actions. You can double-click and right-click objects in the graphic area and move the mouse over nodes, cards, and ports to view popup status information.

CTC Menu and Toolbar Options

The CTC window menu bar and toolbar provide primary CTC functions. Table A-3 shows the actions that are available from the CTC menu and toolbar.

Table A-3 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node		Adds a node to the current session. See the "DLP-A62 Add a Node to the Current Session or Login Group" task on page 3-28.
	Delete Selected Node		Deletes a node from the current session.
	Lock CTC		Locks CTC without closing the CTC session. A user name and password are required to open CTC.
	Print		Prints CTC data. See the "DLP-A515 Print CTC Data" task on page 9-2.
	Export		Exports CTC data. See the "DLP-A516 Export CTC Data" task on page 9-4.
	Exit	—	Closes the CTC session.
Edit	Preferences		Displays the Preferences dialog box, which shows the following tabs: • General—Allows you to change event defaults and manage preferences. • Login Node Groups—Allows you to create login node groups. See the "DLP-A61 Create Login Node Groups" task on page 3-27. • Map—Allows you to customize the network view. See the "DLP-A145 Change the Network View Background Color" task on page 12-11 and the "DLP-A268 Apply a Custom Network View Background Map" task on page 12-12. • Circuit—Allows you to change the color of circuit spans. See the "DLP-A232 Change Active and Standby Span Color" task on page 11-15. • Firewall—Sets the Internet Inter-ORB Protocol (IIOP) listener ports for access to the ONS 15454 through a firewall. See the "NTP-A27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-19. • JRE—Allows you to select another Java Runtime Environment (JRE) version. See the "DLP-A431 Change the JRE Version" task on page 3-29.

Table A-3 CTC Menu and Toolbar Options (continued)

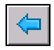
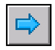
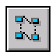
Menu	Menu Option	Toolbar	Description
View	Go To Previous View		Displays the previous CTC view.
	Go To Next View		Displays the next CTC view. Available only after you navigate to a previous view. Go to Previous View and Go to Next View are similar to forward and backward navigation in a web browser.
	Go To Parent View		References the CTC view hierarchy: network view, node view, and card view. In card view, this command displays the node view; in node view, the command displays network view. Not available in network view.
	Go To Selected Object View		Displays the object selected in the CTC window.
	Go To Home View		Displays the login node in node view.
	Go To Network View		Displays the network view.
	Go To Other Node		Displays a dialog box allowing you to type in the node name or IP address of a a network node that you want to view.
	Show Status Bar	—	Click this item to display or hide the status bar at the bottom of the CTC window.
	Show Tool Bar	—	Click this item to display or hide the CTC toolbar.

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Circuits	—	Displays the following options: • Repair Circuits—Repairs incomplete circuits following replacement of the ONS 15454 alarm interface panel (AIP). Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information. • Set Path Selector Attributes—Allows you to edit path protection circuit path selector attributes. See the "DLP-A233 Edit Path ProtectionCircuit Path Selectors" task on page 11-16. • Set Circuit State—Allows you to change a circuit state. See the "DLP-A230 Change a Circuit State" task on page 11-13. • Convert CTC Circuits to TL1 Cross Connects—If a cross-connect in a circuit gets deleted, this menu option allows a user to repair a circuit by separating an incomplete CTC circuit into TL1 cross-connects. Then, the user can replace the missing cross-connect. See the "NTP-A417 Upgrade TL1 Cross-Connects to CTC Circuits" procedure on page 11-23. • Upgrade TL1 Cross Connects to CTC Circuits—Allows you to convert TL1 cross-connects to CTC circuits. See the "NTP-A416 Convert a CTC Circuit to TL1 Cross-Connects" procedure on page 11-22. • Roll Circuit—Allows you to reroute live traffic without interrupting service. This feature requires a Cisco ONS 15600 on your network. Refer to the *Cisco ONS 15600 Procedure Guide.* • Delete Rolls —This feature requires an ONS 15600 on your network. Refer to the *Cisco ONS 15600 Procedure Guide.*
	Overhead Circuits	—	Displays the Repair IP Tunnels option, which fixes circuits that are in the INCOMPLETE state as a result of node IP address changes. See the "DLP-A336 Repair an IP Tunnel" procedure on page 11-20.
	Manage VLANs	—	Displays a list of VLANs that have been created and allows you to delete VLANS. See the "DLP-A335 Delete VLANS" task on page 8-65.
	Open TL1 Connection		Displays the TL1 session dialog box so you can create a TL1 session to a specific node. Refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.
	Open IOS Connection		Displays the IOS command line interface dialog box if an IOS capable card (ML1000-2 or ML100T-12) is installed in the node. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
Help	Contents and Index	—	Displays the online help window.
	Manage Help	—	Displays the versions of online help loaded on your computer.
	About CTC	—	Displays the software version and the nodes in the CTC session.
—	Network View	—	Displays the selected network view. The network view drop-down menu has three options: DWDM, TDM, or All. If you choose DWDM, DWDM and hybrid nodes appear on the network view map. If you choose TDM, TDM and hybrid nodes appear on the network view map. If you choose All, every node on the network appears on the network view map.

Table A-3 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
—	—		Decreases the size of the map area in network view (toolbar only).
—	—		Increases the size of the map area in network view (toolbar only).
—	—		Increases the size of a selected area of the map in network view (toolbar only).
—	—	 	Opens the CTC Alerts dialog box, which shows the status of certain CTC background tasks. When the CTC Alerts toolbar icon contains a red triangle, unread notifications exist. When there are no unread notifications, the CTC Alerts toolbar icon contains a gray triangle (see the Toolbar column left for comparison). Notifications include: • Network disconnection • Send-PDIP inconsistency—CTC discovers a new node that does not have a SEND-PDIP setting consistent with the login node • Circuit deletion status—Reports when the circuit deletion process completes if you choose "Notify when complete" as described in the "NTP-A278 Modify and Delete Overhead Circuits" procedure on page 11-19. The CTC Alerts window always reports circuit deletion errors. • Conditions retrieval error • Software download failure You can save a notification by clicking the Save button in the CTC Alerts dialog box and navigating to the directory where you want to save the text file. By default, the CTC Alerts dialog box opens automatically. To disable automatic popup, see the "DLP-A327 Configure the CTC Alerts Dialog for Automatic Popup" task on page 3-30.

CTC Mouse Options

In addition to the CTC menu bar and toolbar, you can invoke actions by double-clicking CTC window items with your mouse, or by right-clicking an item and selecting actions from shortcut menus. Table A-4 lists the CTC window mouse shortcuts.

Table A-4 CTC Window Mouse Shortcuts

Technique	Description
Double-click	• Node in network view—Displays the node view. • Card in node view—Displays the card view. • Alarm/Event—Displays the object that raised the alarm or event. • Circuits—Displays the Edit Circuit window.
Right-click	• Network view graphic area—Displays a menu that you can use to create a new domain; change the position and zoom level of the graphic image; save the map layout (if you have a Superuser security level); reset the default layout of the network view; set, change, or remove the background image and color; and save or reset the node position. • Node in network view—Displays a menu that you can use to open the node, reset the node icon position to the longitude and latitude set on the Provisioning > General tab, delete the node, fix the node position for auto layout, provision circuits, provision channels, and update circuits or channels with a new node. • Span in network view—Displays a menu that you can use to view information about the span's source and destination ports, the protection scheme, and the optical or electrical level. You can display the Circuits on Spans dialog box, which displays additional span information and allows you to perform path protection protection switching. You can also perform span upgrades from this menu. • Card in node view—Displays a menu that you can use to open, delete, reset, and change cards. The card that you choose determines the commands that appear. • Card in card view—Displays a menu that you can use to reset the card, or go to the parent view (node view). • Empty slot in node view—Displays a menu with cards that you can choose to preprovision the slot.
Move mouse cursor	• Over node in network view—Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range. • Over span in network view—Displays circuit (node, slot, port) bandwidth and protection information. For DWDM spans, the optical direction and optical ring ID appear. If the span terminates on the trunk port of a transponder card (TXP/MXP), the associated DWDM wavelength also appears. • Over card in node view—Displays card type, card status, and alarm profile status. For DWDM cards, the number of bands or channels also appear, depending on the card type. • Over card port in node view—Displays card name, port state, and alarm profile status. • Over card port in card view—Displays port state, protection status (if applicable), and alarm profile status. For DWDM cards, the port number is labeled as channel, band, or line depending on the card type along with the port state and alarm profile status.

Node View Shortcuts

Table A-5 shows actions on ONS 15454 cards that you can perform by moving your mouse over the CTC window.

Table A-5 Node View Card-Related Shortcuts

Action	Shortcut
Display card information	In node view, move your mouse over cards in the graphic to view tooltips with the card type, card present or card provisioned but not present, the highest level of alarm (if any), and the alarm profile used by the card.
Open, reset, or delete a card	In node view, right-click a card. Choose **Open** to display the card in card view, **Delete** to delete it, or **Reset** to reset the card.
Preprovision a slot	In node view, right-click an empty slot. Choose the card type that you want to provision the slot from the shortcut menu.
Change a card	In node view, right-click an OC-N card or a DS3 card, and choose **Change Card**. In the Change Card dialog box, choose the card type. Change card retains all card provisioning, including DCC terminations, protection, circuits, and ring.

Network View Tasks

Right-click the network view graphic area or a node, span, or domain to display shortcut menus. Table A-6 lists the actions that are available from the network view.

Table A-6 Network Management Tasks in Network View

Action	Task
Open a node	Any of the following: • Double-click a node icon. • Right-click a node icon and choose **Open Node** from the shortcut menu. • Click a node and choose **Go To Selected Object View** from the View menu. • From the View menu, choose **Go To Other Node**. Choose a node from the Select Node dialog box. • Double-click a node alarm or event in the Alarms or History tab.
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.
Reset node icon position	Right-click a node and choose **Reset Node Position** from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tab in node view.
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and choose the node where you want to provision the circuit. For circuit creation procedures, see Chapter 8, “Create Circuits and VT Tunnels.”

Table A-6 Network Management Tasks in Network View (continued)

Action	Task
Update circuits with new node	Right-click a node and choose **Update Circuits With New Node** from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link end point	Right-click a span. From the shortcut menu, choose **Go To [node/slot/port]** for the drop port you want to view. CTC displays the card in card view.
Display span properties	Do any of the following: • Move mouse over a span; the properties appear near the span. • Click a span; the properties appear in the upper left corner of the window. • Right-click a span; the properties appear at the top of the shortcut menu.
Perform a path protection switch for an entire span	Right-click a network span and click **Circuits**. In the Circuits on Span dialog box, switch options appear in the UPSR Span Switching field.
Display DWDM span properties	Right-click a DWDM network span and click **Circuits**. The OCHNC channel, optical direction, and circuit appear.
Upgrade a span	Right-click a span and choose **Upgrade Span** from the shortcut menu. **Note** For detailed span upgrade information and instructions, see Chapter 14, "Upgrade Cards and Spans."

Table Display Options

Right-clicking a table column displays a menu. Table A-7 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

Table A-7 Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Left-click while dragging the header separator to the right or left.	—
Rearrange column order	Left-click while dragging the column header to the right or left.	—
Reset column order	—	Choose **Reset Columns Order/Visibility**.
Hide column	—	Choose **Hide Column**.
Show column	—	Choose **Show Column >** *column_name*.
Display all hidden columns	—	Choose **Reset Columns Order/Visibility**.
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending).	Choose **Sort Column**.

Table A-7 Table Display Options (continued)

Task	Click	Right-Click Shortcut Menu
Sort table (secondary sorting keys)	Press the **Shift** key and simultaneously click the column header.	Choose **Sort Column (incremental)**.
Reset sorting	—	Choose **Reset Sorting**.
View table row count	—	View the number listed next to “Row Count,” it is the last item on the shortcut menu.

Equipment Inventory

In node view, the Inventory tab displays information about the ONS 15454 equipment, including:

- Delete button—After highlighting a card with your mouse, use this button to delete the card from node view.
- Reset button—After highlighting a card with your mouse, use this button to reset the card.
- Location—Identifies where the equipment is installed, either chassis or slot number.
- Eqpt Type—Displays the type of equipment but not the specific card name, for example, OC-12 or DS-1.
- Actual Eqpt Type—Displays the actual equipment type, for example, OC12 IR/STM4 SH 1310.
- HW Part #—Displays the hardware part number; this number is printed on the top of the card or equipment piece.
- HW Rev—Displays the hardware revision number.
- Serial #—Displays the equipment serial number; this number is unique to each card.
- CLEI Code—Displays the Common Language Equipment Identifier code.
- Firmware Rev—Displays the revision number of the software used by the ASIC chip installed on the ONS 15454 card.
- Product ID—Displays the manufacturing product identifier for a hardware component, such as a fan tray, chassis, or card. The Product ID column displays “N/A” for equipment existing before Software Release 4.6.
- Version ID—Displays the manufacturing version identifier for a fan tray, chassis, or card. The Version ID column displays “N/A” for equipment existing before Software Release 4.6.

APPENDIX B

Specifications

This appendix contains hardware and software specifications for the ONS 15454.

Bandwidth

The ONS 15454 has the following bandwidth specifications:

- Total bandwidth: 240 Gbps
- Data plane bandwidth: 160 Gbps
- SONET plane bandwidth: 80 Gbps

Configurations

The ONS 15454 can be configured as follows:

- Two-fiber path protection
- Path protected mesh network (PPMN)
- Two-fiber bidirectional line switch ring (BLSR)
- Four-fiber BLSR
- Add-drop multiplexer
- Terminal mode
- Regenerator mode
- Hubbed rings
- Multihubbed rings
- Point-to-point
- Linear
- Linear with optical add/drop multiplexing (OADM)

Cisco Transport Controller

Cisco Transport Controller (CTC), the ONS 15454 craft interface software, has the following specifications:

- 10 BaseT
- TCC2 access: RJ-45 connector
- Backplane access: LAN pin field

External LAN Interface

The ONS 15454 external LAN interface has the following specifications:

- 10 BaseT Ethernet
- Backplane access: LAN pin field

TL1 Craft Interface

The ONS 15454 TL1 craft interface has the following specifications:

- Speed: 9600 bps
- TCC2 access: EIA/TIA-232 DB-9 type connector
- Backplane access: CRAFT pin field

Modem Interface

The ONS 15454 modem interface has the following specifications:

- Hardware flow control
- TCC2: EIA/TIA-232 DB-9 type connector

Alarm Interface

The ONS 15454 alarm interface has the following specifications:

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: 0.045 mm, –48 V, 50 mA
- Backplane access: Alarm pin fields

EIA Interface

The ONS 15454 EIA interface has the following specifications:

- SMB: AMP #415504-3 75-ohm, 4-leg connectors
- BNC: Trompeter #UCBJ224 75-ohm 4 leg connector (King or ITT are also compatible)
- AMP Champ: AMP#552246-1 with #552562-2 bail locks

BITS Interface

The ONS 15454 BITS interface has the following specifications:

- 2 DS-1 building integrated timing supply (BITS) inputs
- 2 derived DS-1 outputs
- Backplane access: BITS pin field

System Timing

The ONS 15454 has the following system timing specifications:

- Stratum 3 per Telcordia GR-253-CORE
- Free running accuracy: ± 4.6 ppm
- Holdover stability: 3.7 $x10^{-7}$/day, including temperature (< 255 slips in first 24 hours)
- Reference: External BITS, line, internal

Power Specifications

System Power

The ONS 15454 has the following power specifications:

- Input power: –48 VDC
- Power consumption: 55 W (fan tray only); 650 W (maximum draw w/cards)
- Power requirements: –40.5 to –57 VDC
- Power terminals: #6 Lug
- ANSI shelf: 100-A fuse panel (minimum 30 A fuse per shelf)
  HD shelf: 100-A fuse panel (minimum 35 A fuse per shelf)

Cards

Table B-1 provides power consumption information for the ONS 15454 cards.

Table B-1 Individual Card Power Requirements

Card Type	Card Name	Watts	Amperes	BTU/Hr.
Control Cards	TCC2	19.20	0.4	66.8
	XC	29.00	0.60	99
	XCVT	34.40	0.72	117.46
	XC10G	48	1	163.68
	AIC	6.01	0.12	20.52
	AIC-I	4.8	0.1	15.3
	AEP	3	(from +5 VDC from AIC-I)	10.2
Electrical Cards	EC1-12	36.60	0.76	124.97
	DS1-14	12.60	0.26	43.02
	DS1N-14	12.60	0.26	43.02
	DS3-12	38.20	0.79	130.43
	DS3N-12	38.20	0.79	130.43
	DS3i-N-12	30	0.63	102.4
	DS3-12E	26.80	0.56	91.51
	DS3N-12E	26.80	0.56	91.51
	DS3XM-6 Transmux	20	0.42	68

Table B-1 Individual Card Power Requirements (continued)

Card Type	Card Name	Watts	Amperes	BTU/Hr.
Optical Cards	OC3 IR 4	19.20	0.40	65.56
	OC3 IR 4/STM1 SH 1310	19.20	0.40	65.56
	OC3 IR 4/STM1SH 1310-8	26.00	0.48	78.5
	OC12 IR 1310	10.90	0.23	37.22
	OC12 LR 1310	9.28	0.2	31.68
	OC12 LR 1550	9.28	0.2	31.68
	OC12 LR/STM4 LH 1310	9.00	0.2	31.68
	OC12 LR/STM4 LH 1550	9.28	0.2	31.68
	OC12 IR/STM4 SH 1310-4	35.60	0.74	121.6
	OC48 IR 1310	32.20	0.67	109.94
	OC48 LR 1550	26.80	0.56	91.50
	OC48 IR/STM16 SH AS 1310	37.20	0.77	127.01
	OC48 LR/STM16 LH AS 1550	37.20	0.77	127.01
	OC48 ELR/STM16 EH 100 GHz	31.20	0.65	106.53
	OC48 ELR 200 GHz	31.20	0.65	106.53
	OC192 SR/STM64 IO H 1310	41.80	.90	132.00
	OC192 IR/STM64 SH 1550	48.00	1.00	163.68
	OC192 LR/STM64 LH 1550	41.80	.9	132.00
	OC192 LR/STM64 LH 15xx.xx	62.40	1.30	214.00
	TXP_MR_10G	35.00[1]	0.73	119.5
	MXP_2.5G_10G	50[1]	1.04	170.7
	TXP_MR_2.5G	35.00[2]	0.73	119.5
	TXPP_MR_2.5G	50[1]	1.04	170.5

Table B-1 Individual Card Power Requirements (continued)

Card Type	Card Name	Watts	Amperes	BTU/Hr.
DWDM Cards	OSCM	Nominal 23 Maximum 26	Nominal 0.48 Maximum 0.54	Nominal 78.48 Maximum 88.71
	OSC-CSM	Nominal 24 Maximum 27	Nominal 0.5 Maximum 0.56	Nominal 81.89 Maximum 92.12
	OPT-PRE	Minimum 25 Nominal 30 Maximum39	Minimum 0.52 Nominal 0.5 Maximum 0.81	Minimum 85.3 Nominal 102.36 Maximum 88.71
	OPT-BST	Nominal 30 Maximum 39	Nominal 0.63 Maximum 0.81	Nominal 102.36 Maximum 88.71
	32 MUX-O	Nominal 16 Maximum 25	Nominal 0.33 Maximum 0.52	Nominal 54.59 Maximum 85.3
	32 DMX-O	Nominal 16 Maximum 25	Nominal 0.33 Maximum 0.52	Nominal 54.59 Maximum 85.3
	4MD-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
	AD-1C-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
	AD-2C-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
	AD-4C-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
	AD-1B-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
	AD-4B-xx.x	Nominal 17 Maximum 25	Nominal 0.35 Maximum 0.52	Nominal 58.0 Maximum 85.3
Ethernet Cards	E100T-12	65	1.35	221.93
	E1000-2	53.50	1.11	182.67
	E100T-G	65	1.35	221.93
	E1000-2-G	53.50	1.11	182.67
	G1000-4	63.00	1.31	215.11
	ML100T-12	53	1.10	181.0
	ML1000-2	49 (incl. SFPs)	1.02	167.3
Fibre Channel	FC_MR-4	60[1]	1.25	212.00

1. Calculated power; measured power was not available at the time of publication.
2. Calculated power; measured power was not available at the time of publication.

Environmental Specifications

System

The ONS 15454 has the following environmental specifications:

- Operating temperature: 0 to +55 degrees Celsius; –40 to +65 degrees Celsius with industrial temperature rated cards
- Operating humidity: 5 to 95%, noncondensing

Cards

Table B-2 provides temperature ranges and product names for ONS 15454 cards.

Note The I-Temp symbol is displayed on the faceplate of an I-Temp compliant card. A card without this symbol is C-Temp compliant.

Table B-2 Card Temperature Ranges and Product Names

Card Type	Card Name	C-Temp Product Name (32 to 131 degrees Fahrenheit, 0 to +55 degrees Celsius)	I-Temp Product Name (–40 to 149 degrees Fahrenheit, –40 to +65 degrees Celsius)
Control Cards			
	TCC2	—	15454-TCC2
	XC	15454-XC	15454-XC-T
	XCVT	15454-XC-VT	15454-XC-VT-T
	XC10G	15454-XC-10G	—
	AIC	15454-AIC	15454-AIC-T
	AIC-I	—	15454-AIC-I
	AEP	—	15454-AEP
Electrical	EC1-12	15454-EC1-12	15454-EC1-12-T
	DS1-14	15454-DS1-14	15454-DS1-14-T
	DS1N-14	15454-DS1N-14	15454-DS1N-14-T
	DS3-12	15454-DS3-12	15454-DS3-12-T
	DS3N-12	15454-DS3N-12	15454-DS3N-12-T
	DS3i-N-12	15454-DS3i-N-12	—
	DS3-12E	—	15454-DS3-12E-T
	DS3N-12E	—	15454-DS3N-12E-T
	DS3XM-6 (Transmux)	15454-DS3XM-6	15454-DS3XM-6-T

Table B-2 Card Temperature Ranges and Product Names (continued)

Card Type	Card Name	C-Temp Product Name (32 to 131 degrees Fahrenheit, 0 to +55 degrees Celsius)	I-Temp Product Name (–40 to 149 degrees Fahrenheit, –40 to +65 degrees Celsius)
Optical	OC3 IR 4/STM1 SH 1310	15454-OC34IR1310	15454-OC34I13-T
	OC3 IR/STM1 SH 1310-8	15454-OC3I8-1310	—
	OC12 IR/STM4 SH 1310	15454-OC121IR1310	15454-OC121I13-T
	OC12 LR/STM4 LH 1310	15454-OC121LR1310	15454-OC121L13-T
	OC12 LR/STM4 LH 1550	15454-OC121LR1550	15454-OC121L15-T
	OC12 IR/STM4 SH 1310-4	15454-OC12I4-1310	—
	OC48 IR 1310	15454-OC481IR1310	—
	OC48 LR 1550	15454-OC481LR1550	—
	OC48 IR/STM16 SH AS 1310	15454-OC481IR1310A	—
	OC48 LR/STM16 LH AS 1550	15454-OC481LR1550A	—
	OC48 ELR/STM16 EH 100 GHz	15454-OC48E-1-xx.xx (all wavelengts)	—
	OC48 ELR/STM16 EH 200 GHz	15454-OC48E-xx.xx (all wavelengths)	—
	OC 192 SR/STM64 IO 1310	15454-OC192IO1310	—
	OC192 IR/STM64 SH 1550	15454-OC192IR1550	—
	OC192 LR/STM64 LH 1550	15454-OC192LR1550	—
	OC192 LR/STM64 LH ITU 15xx.xx	15454-OC192LR15xx	—
	TXP_MR_10G	15454-TXPMR10G	—
	MXP_2.5G_10G	15454-MXP2.5G10G	—
	TXP_MR_2.5G	15454-2.5GMRTXP	—
	TXPP_MR_2.5G	15454-2.5GMRTXP-P	—

Table B-2 Card Temperature Ranges and Product Names (continued)

Card Type	Card Name	C-Temp Product Name (32 to 131 degrees Fahrenheit, 0 to +55 degrees Celsius)	I-Temp Product Name (–40 to 149 degrees Fahrenheit, –40 to +65 degrees Celsius)
DWDM	OSCM	15454-OSCM	—
	OSC-CSM	15454-OSC-CSM	—
	OPT-PRE	15454-OPT-PRE	—
	OPT-BST	15454-OPT-BST	—
	32 MUX-O	15454-32 MUX-O	—
	32 DMX-O	15454-32 DMX-O	—
	4MD-xx.x	15454-4MD-xx.x	—
	AD-1B-xx.x	15454-AD-1B-xx.x	—
	AD-4B-xx.x	15454-AD-4B-xx.x	—
	AD-1C-xx.x	15454-AD-1C-xx.x	—
	AD-2C-xx.x	15454-AD-2C-xx.x	—
	AD-4C-xx.x	15454-AD-4C-xx.x	—
Fibre Channel	FC_MR-4	15454-FC_MR-4	—

Dimensions

The ONS 15454 shelf assembly has the following dimensions:

- Height: 18.5 in. (40.7 cm)
- Width: 19 or 23 in. (41.8 or 50.6 cm) with mounting ears attached
- Depth: 12 in. (26.4 cm) (5 in. or 12.7 cm projection from rack)
- Weight: 55 lb (24.947 kg) empty

GLOSSARY

Numerics

1:1 protection

An electrical card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot (DS-1 and DS-3 speeds). If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts to the working card.

1+1 protection

An optical (OC-N) card protection scheme that pairs a single working port/card with a single dedicated protect port/card. All OC-N cards can use this protection type (OC-3, OC-12, OC-48, and OC-192 speeds).

1:N protection

An electrical card protection scheme that allows a single protect card to provide protection for several working cards (DS-1 and DS-3 speeds). If a working card fails, the traffic from the working card switches to the protect card.When the failure on the working card is resolved, traffic reverts to the working card.

10BaseT

Standard 10 Mbps local area network over unshielded twisted pair copper wire.

100BaseT

Standard 100 Mbps local ethernet network.

100BaseTX

Specification of 100BaseT that supports full duplex operation.

A

Access drop

Points where network devices can access the network.

ACO

Alarm cutoff.

Active card

A card that is working or carrying traffic. A card provisioned as working can be an active card or, after a protection switch, a protect card can be an active card.

ACT/STBY

Active/Standby.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the portion that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

(Add/drop multiplexers). Linear ADMs allow signals to be added to a SONET span or dropped from a SONET span. An ADM has three or more nodes.

Agent

1. Generally, software that processes queries and returns replies on behalf of an application.
2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

AIC

Alarm Interface Controller.

AID

(Access Identifier). An access code used in TL1 messaging that identifies and addresses specific objects within the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and others. See also *TID*.

AIP

Alarm Interface Panel.

AIS

Alarm Indication Signal.

AIS-L

Line Alarm Indication Signal.

AMI

(Alternate Mark Inversion). Line-code format used on T1 circuits that transmits ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

ANSI

American National Standards Institute.

APS

(Automatic Protection Switching). SONET switching mechanism that routes traffic from working lines to protect lines if a line card failure or fiber cut occurs.

ARP

Address Resolution Protocol.

APSB

Alarm Protection Switching Byte.

ATAG

(Autonomous Message Tag). ATAG is used for TL1 message sequencing. See also *CTAG*.

ATM

Asynchronous Transfer Mode.

AWG

American Wire Gauge

B

B8ZS

(Binary 8-zero Substitution). A line-code type, used on T1 circuits, that substitutes a special code whenever 8 consecutive zeros are sent over the link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream. Sometimes called bipolar 8-zero substitution.

Backbone

The part of the network that carries the heaviest traffic or joins LANs together.

BER

(Bit Error Rate). Ratio of received bits that contain errors.

BIP

Bit Interleaved Parity.

Bit rate

Speed at which bits are transmitted, usually expressed in bits per second.

BITS

(Building Integrated Timing Supply). A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

BLSR

(Bidirectional Line Switched Ring). SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber. See also *Path Protection*.

Blue band

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 SDH operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

BNC

Bayonet Neill-Concelman (coaxial cable bayonet-locking connector).

BPDU

Bridge Protocol Data Unit.

Bridge

Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame. See also *MAC address*.

Broadcast

Data packet that will be sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

Broadcast address

Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones. See also *MAC address.*

Broadcast storm

Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Bus

Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

C

C2 byte

The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. See also *SONET.*

CAT 5

Category 5 (cabling).

CCITT

Comité Consultatif International Télégraphique et Téléphoniques. (Formerly ITU.)

CEO

Central Office Environment.

CEV

Controlled Environment Vaults.

CLEI

Common Language Equipment Identifier code.

CLNP

Correctionless Network Protocol.

cm

Centimeter.

CMIP

Common Management Information Protocol.

COE

Central Office Environment.

Collision

In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

Concatenation

A mechanism for allocating contiguous bandwidth for payload transport. Through the use of Concatenation Pointers, multiple OC-1s can be linked together to provide contiguous bandwidth through the network, from end to end.

CORBA

Common Object Request Broker Architecture.

CPE

Customer Premise Environments.

Crosspoint

A set of physical or logical contacts that operate together to extend the speech and signal channels in a switching network.

CTAG

(Correlation Tag). A unique identifier given to each input command by the TL1 operator. When the ONS 15454 system responds to a specific command, it includes the command's CTAG in the reply. This eliminates discrepancies about which response corresponds to which command. See also *ATAG*.

CTC

(Cisco Transport Controller). A Java-based graphical user interface (GUI) that allows operations, administration, maintenance, and provisioning (OAM&P) of the ONS 15454 using an Internet browser.

CTM

(Cisco Transport Manager). A Java-based network management tool used to support large networks of Cisco 15000-class

D

DCC

(Data Communications Channel). Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCC can be located in SDCC or LDCC. See also *LDCC* and *SDCC*.

DCN

Data Communications Network.

DCS

Distributed Communications System.

Default router

If the ONS 15454 must communicate with a device on a network to which the ONS 15454 is not connected, packets are sent to this router to be distributed.

Demultiplex

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. Compare *Multiplexing*.

Destination

The endpoint where traffic exits an ONS 15454 network. Endpoints can be paths (STS or STS/VT for optical card endpoints), ports (for electrical circuits, such as DS1, VT, DS3, STS), or cards (for circuits on DS1 and Ethernet cards). See also STS, and *VT*.

DRAM

Dynamic Random-Access Memory.

Drop

See *Destination*.

DS-1

Digital Signal Level One.

DS1-14

Digital Signal Level One (14 ports).

DS1N-14

Digital Signal Level One (N-14 ports).

DS-3

Digital Signal Level Three.

DS3-12

Digital Signal Level Three (12 ports).

DS3N-12

Digital Signal Level Three (N-12 ports).

DS3XM-6

Digital Service, level 3 Trans-Multiplexer 6 ports.

DSX

(Digital Signal Cross-Connect Frame). A manual bay or panel where different electrical signals are wired. A DSX permits cross-connections by patch cords and plugs.

DWDM

(Dense Wave Division Multiplexing). A technology that increases the information carrying capacity of existing fiber optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.

DWDM Node

An ONS 15454 running Software Release 4.5. See *Non-DWDM Node*.

E

EDFA

(Erbium Doped Fiber Amplifier). A type of fiber optical amplifier that transmits a light signal through a section of erbium-doped fiber and amplifies the signal with a laser pump diode. EDFA is used in transmitter booster amplifiers, in-line repeating amplifiers, and in receiver preamplifiers.

EFCA

Electrical Facility Connection Assembly.

EFT

Electrical Fast Transient/Burst.

EIA

(Electrical Interface Assemblies). Provides backplane connection points for the DS-1, DS-3, and EC-1 cards.

ELR

Extended Long Reach.

EMC

Electromagnetic compatibility.

EMI

(Electromagnetic Interference). Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

EML

Element Manager Layer.

EMS

Element Management System.

Envelope

The part of messaging that varies in composition from one transmittal step to another. It identifies the message originator and potential recipients, documents its past, directs its subsequent movement by the Message Transfer System (MTS), and characterizes its content.

EOW

(Engineered Orderwire). A permanently connected voice circuit between selected stations for technical control purposes.

ERDI

Enhanced Remote Defect Indicator.

ES

Errored Seconds.

ESD

Electrostatic Discharge.

ESF

Extended Super Frame.

Ethernet switch

A type of Ethernet LAN device that increases aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously shared LAN segments into multiple networks with fewer stations per network.

ETSI

European Telecommunications Standards Institute.

Extended SNCP

(Extended Subnetwork Connection Protection). Extended SNCP extends the protection scheme of a subnetwork connection protection ring (SNCP) beyond the basic ring configuration to the meshed architecture of several interconnecting rings. See *SNCP*.

External timing reference

A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

F

Falling threshold

A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

FC

Failure count.

FDDI

(Fiber Distributed Data Interface). LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

FE

Frame Bit Errors.

FG1

Frame Ground #1 (pins are labeled "FG1," "FG2," etc.)

FMEC

Front Mount Electrical Connection.

Frame

Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

FSB

Field Service Bulletin.

G

Gateway

An electronic repeater device that intercepts and steers electrical signals from one network to another.

GBIC

(Gigabit Interface Converter). A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GR-153-CORE

General Requirements #253 Council of Registrars.

GR-1089

General Requirements #1089.

GUI

Graphical User Interface.

H

Hard reset

The physical removal and insertion of a TCC+ card, also known as reseating a card or performing a card pull.

HDLC

(High-Level Data Link Control). Bit-oriented, synchronous, data-link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Hop

A hop is a way to quantify the 'length' of a network route to decide which redundant route is selected. Typically each path segment through a routing network device is considered one hop. For example, if an ENE is connected to a GNE that is connected to a router, the ENE has two hops to the router—one from itself to the GNE and a second from the GNE to the router. To ensure that a certain route is used only when all other routes are exhausted, assign it an unusually high hop count.

Host number

Part of IP address used to address an individual host within the network or subnetwork.

Hot swap

The process of replacing a failed component while the rest of the system continues to function normally.

I

IEC

1. InterExchange Carrier.
2. International Electrotechnical Commission.

IEEE

Institute of Electrical and Electronics Engineers.

IETF

Internet Engineering Task Force.

Input alarms

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

I/O

Input/Output.

IP

(Internet Protocol). Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IPPM

Intermediate-Path Performance Monitoring.

IP address

32-bit address assigned to host using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.

ITU-T

International Telecommunication Union - Telecommunication Standards Sector.

J

JRE

Java Runtime Environment.

K

K bytes

Automatic protection-switching bytes located in the SONET line overhead and monitored by equipment for an indication to switch to protection.

L

LAN

(Local Area Network). High-speed, low error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LCD

(Liquid Crystal Display). An alphanumeric display using liquid crystal sealed between two pieces of glass. LCDs conserve electricity.

LDCC

Line Data Communication Channel.

Line layer

Refers to the segment between two SONET devices in the circuit. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization. Sometimes called a maintenance span.

Line terminating equipment (LTE)

Refers to line cards which terminate the line signal in the ONS 15454.

Line timing mode

A node that derives its clock from the SONET lines.

Link budget

The difference between the output power and receiver power of an optical signal expressed in dB. Link refers to an optical connection and all of its component parts (optical transmitters, repeaters, receivers, and cables).

Link integrity

The network communications channel has link integrity if it is intact.

Lock Out

A method of switching traffic from one card to another, or one span to another (BLSRs), that prevents traffic from reverting to the card or span with the lock out applied. The lock out overrides other manual switching connections (force, manual, and exercise).

LOF

Loss of Frame.

Loopback test

Test that sends signals then directs them back toward their source from some point along the communications path. Loopback tests are often used to test network interface usability.

LOP

Loss of Pointer.

LOS

Loss of Signal.

LOW

(Local Orderwire). A communications circuit between a technical control center and selected terminal or repeater locations.

LTE

Line Terminating Equipment.

LVDS

Low-Voltage Differential Signal.

M

MAC

Media Access Control.

MAC address

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as the hardware address, MAC-layer address, and physical address.

Maintenance user

A security level that limits user access to maintenance options only. See also *Superuser*, *Provisioning User*, and *Retrieve User.*

Managed device

A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers.

Managed object

In network management, a network device that can be managed by a network management protocol. Sometimes called an MIB object.

Mapping

A logical association between one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

Mbps

Megabits per second.

MBps

Megabytes per second.

MHz

Megahertz.

MIB

(Management Information Base). Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIME

Multipurpose Internet Mail Extensions.

MS

Multiplex Section.

MS-FERF

Multiplex Section Far-end Receive Failure.

MSP

Multiplex Section Protection.

MS-SPRing

(Multiplex Section Shared Protection Ring.) SDH ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically rerouted onto the protection fiber.

Multicast

Single packets copied by the network and sent to a specific subset of network addresses.

Multiplex payload

Generates section and line overhead, and converts electrical/optical signals when the electrical/optical card is transmitting.

Multiplexing

Scheme that allows multiple signals to be transmitted simultaneously across a single physical channel. Compare *Demultiplex*.

Mux/Demux

Multiplexer/Demultiplexer.

Muxed

Multiplexed. See *Multiplexing*.

N

NE

(Network Element). In an Operations Support System, a single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

NEBS

Network Equipment-Building Systems.

NEL

Network Element Layer.

Network number

Part of an IP address that specifies the network where the host belongs.

NML

Network Management Layer.

NMS

(Network Management System). System that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.

Node

In this manual the term “node” usually refers to an ONS 15454. A node is the endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network. Node is sometimes used generically to refer to any entity that can access a network.

Non-DWDM Node

An ONS 15454 running Software Release 4.1 or earlier. Nodes running Software Release 4.5 are termed “DWDM nodes.”

O

OAM&P

(Operations, Administration, Maintenance, and Provisioning). Provides the facilities and personnel required to manage a network.

OC

Optical carrier.

OOS AS

Out of Service Assigned.

Optical amplifier

A device that amplifies an optical signal without converting the signal from optical to electrical and back again to optical energy.

Optical receiver

An opto-electric circuit that detects incoming lightwave signals and converts them to the appropriate signal for processing by the receiving device.

Orderwire

Equipment that establishes voice contact between a central office and carrier repeater locations. See *Local orderwire*.

OSI

Open Systems Interconnection.

OSPF

Open Shortest Path First.

OSS

Operations Support System.

OSS/NMS

Operations Support System/Network Management System.

Output contacts (controls)

Triggers that drive visual or audible devices such as bells and lights. Output contacts can control other devices such as generators, heaters, and fans.

P

Passive devices

Components that do not require external power to manipulate or react to electronic output. Passive devices include capacitors, resisters, and coils.

Path Layer

The segment between the originating equipment and the terminating equipment. This path segment may encompass several consecutive line segments or segments between two SONET devices.

Payload

Portion of a cell, frame, or packet that contains upper-layer information (data).

PCM

Pulse Code Modulation.

PCMCIA

Personal Computer Memory Card International Association.

PCN

Product Change Notice(s).

PDI-P

STS Payload Defect Indication - Path.

Ping

(Packet internet grouper). ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

Pointer justification

In SONET, the mechanism used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks.

POP

Point of Presence.

PM

Performance Monitoring.

PPMN

(Path-Protected Mesh Network). PPMN extends the protection scheme of a path protection beyond the basic ring configuration to the meshed architecture of several interconnecting rings.

Priority queuing

Routing feature that divides data packets into two queues: one low-priority and one high-priority.

Protect card

A card in a protection pair or scheme that is provisioned as a protect card to the working card. If the working card fails, the protect card becomes active. See also *working card*.

Provisioning user

A security level that allows the user to access only provisioning and maintenance options in CTC. See also *Superuser*, *Maintenance user,* and *Retrieve user*.

PSC

Protection-Switching Count.

PSD

Protection-Switching Duration.

PTE

Path-Terminating Equipment.

Q

Queue

In routing, a backlog of packets waiting to be forwarded over a router interface.

R

RAM

Random Access Memory.

RDI-L

Remote Defect Indication - Line.

Red band

DWDM wavelengths are broken into two distinct bands: red and blue. The red band is the higher frequency band. The red band DWDM cards for the ONS 15454 SDH operate on wavelengths between 1547.72nm and 1560.61nm.

RES

Reserved.

Retrieve user

A security level that allows the user to retrieve and view CTC information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user.*

Revertive switching

A process that sends electrical interfaces (traffic) back to the original working card after the card comes back online.

Rising threshold

The number of occurrences (collisions) that must be exceeded to trigger an event.

RJ-45

Registered Jack #45 (8-pin).

RMA

Return Materials Authorization.

RMON

(Remote Network Monitoring). Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

RS-232

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication).

Rx

Receive.

S

SCI

Serial Communication Interface.

SCL

System Communications Link.

SDCC

Section Data Communication Channel.

SDH

(Synchronous Digital Hierarchy). European standard that defines a set of rate and format standards that are transmitted using optical signals over fiber. SDH is similar to SONET, with a basic SDH rate of 155.52 Mbps. Compare *SONET*.

SEF

Severely Errored Frame.

SELV

Safety Extra-Low Voltage.

SES

Severely Errored Seconds.

SF

Super Frame.

SML

Service Management Layer.

SMF

Single Mode Fiber.

SNCP

(Subnetwork Connection Protection Ring). Path-switched SDH rings that employ redundant, fiber-optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over.

SNMP

(Simple Network Management Protocol). Network management protocol used almost exclusively in TCP/IP networks. SNMP monitors and controls network devices and manages configurations, statistics collection, performance, and security.

SNTP

(Simple Network Time Protocol). Using an SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

Soft reset

A soft reset reloads the operating system, application software, etc., and reboots the TCC+ card. It does not initialize the ONS 15454 ASIC hardware.

SONET

(Synchronous Optical Network). High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

Source

The endpoint where traffic enters an ONS 15454 network. Endpoints can be a path (STS or STS/VT for optical card endpoints), port (for electrical circuits, such as DS1, VT, DS3, STS), or card (for circuits on DS1 and Ethernet cards). See also *STS* and *VT*.

Span

An optical path between two nodes.

Spanning tree

A loop-free subset of a network topology. See also *STA* and *STP*.

SPE

(Synchronous Payload Envelope). A SONET term describing the envelope that carries the user data or payload.

SSM

(Synchronous Status Messaging). A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

STA

(Spanning-Tree Algorithm). An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP*.

Standby card

A card that is not active or carrying traffic. A standby card can be a protect card or, after a protection switch, a working card can be a standby card.

Static route

A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.

STP

1. Shielded Twisted Pair.
2. Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm to enable a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. See also *Spanning tree and STA*.

STS

(Synchronous Transport Signal, used generically when speaking of SONET signals.)

STS-1

(Synchronous Transport Signal Level 1). Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-*n*, where *n* is a multiple of 51.84 Mbps. See also *SONET*.

Subnet mask

32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address*.

Subnetwork

In IP networks, a network confined to a particular subnet address. Subnetworks are networks segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet.

Subtending rings

SONET rings that incorporate nodes that are also part of an adjacent SONET ring.

Superuser

A security level that can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A superuser is usually the network element administrator. See also *Retrieve user*, *Maintenance user*, and *Provisioning user.*

Switching, Span

Span switching occurs when a working span fails. Traffic switches to the protect fibers between the nodes and then returns to the working fibers. Multiple span switches can occur at the same time.

Switching, Ring

Ring switching occurs when a span switch cannot recover traffic, such as when both the working and protect fibers fail on the same span. In a ring switch, traffic is routed to the protect fibers throughout the full ring.

SWS

SONET WAN switch.

SXC

SONET Cross Connect ASIC.

T

T1

T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network using AMI or B8ZS coding. See also *AMI*, *B8ZS*, and *DS-1*.

TAC

Technical Assistance Center.

Tag

Identification information, including a number plus other information.

TBOS

Telemetry Byte-Oriented Serial protocol.

TCA

Threshold Crossing Alert.

TCC+

Timing Communications and Control + Card

TCP/IP

Transmission Control Protocol/Internet Protocol

TDM

(Time Division Multiplexing). Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

TDS

Time-Division Switching.

Telcordia

(Telcordia Technologies, Inc., formerly named Bellcore). Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

TID

(Target Identifier). Identifies the particular network element (in this case, the ONS 15454) where each TL1 command is directed. The TID is a unique name given to each system at installation. See also *AID*.

TL1

Transaction Language 1.

TLS

(Transparent LAN Service). Provides private network service across a SONET backbone.

TMN

Telecommunications Management Network.

Transponder

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength. See also *DWDM*.

Trap

Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold. See also *CTM*.

Tributary

The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low rate signals to form an aggregate higher rate level.

Trunk

Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

TSA

Time-Slot Assignment.

TSI

Time-Slot Interchange.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Tx

Transmit.

U

UAS

Unavailable Seconds.

UDP/IP

User Datagram Protocol/Internet Protocol.

UID

User Identifier.

Unicast

The communication of a single source to a single destination.

Path protection

Path-switched SONET rings that employ redundant, fiber- optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over. See also *BLSR*.

Upstream

Set of frequencies used to send data from a subscriber to the head end.

UTC

Universal-Time Coordinated.

UTP

Unshielded Twisted Pair.

V

VDC

Volts Direct Current.

Virtual fiber

A fiber that carries signals at different rates and uses the same fiber optic cable.

Virtual ring

Entity in a source-route bridging (SRB) network that logically connects two or more physical rings together either locally or remotely. The concept of virtual rings can be expanded across router boundaries.

Virtual wires

Virtual wires route external alarms to one or more alarm collection centers across the SONET transport network.

VLAN

(Virtual LAN). Group of devices located on a number of different LAN segments that are configured (using management software) to communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN

(Virtual Private Network). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level. See also *Tunneling*.

VT

(Virtual Tributary). A structure designed for the transport and switching of sub-DS3 payloads. See also *Tributary.*

VT1.5

Virtual Tributary that equals 1.544 Mbps.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

VT tunnel

VT tunnels allow electrical circuits to pass through ONS 15454 nodes without using ONS 15454 cross-connect card capacity.

W

W

Watts.

WAN

Wide Area Network.

Working card

A card that is provisioned as an active, primary card. Traffic cards in a protection pair are provisioned as working or protect See also *Protect card*.

X

XC

Cross Connect

XCVT

Cross Connect Virtual Tributary.

X.25

Protocol providing devices with direct connections to a packet-switched network.

INDEX

Numerics

A

B

D

E

F

G

H

I

M

N

O

P

Q

R

S

T

U

V