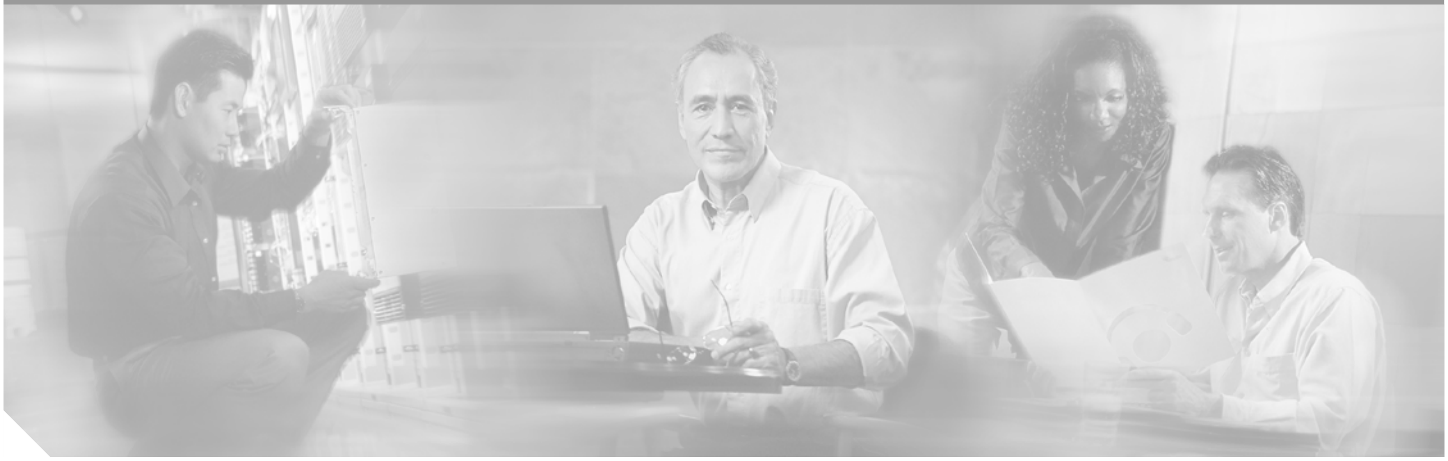


Cisco ONS 15454 Procedure Guide

Product and Documentation Release 3.4
Last Updated: November 10, 2004

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

Text Part Number: 78-14870-01

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cisco ONS 15454 Procedure Guide

CONTENTS

CHAPTER 2

CHAPTER 3

CHAPTER 14

CHAPTER 15

CHAPTER 16

INDEX

FIGURES

TABLES

PROCEDURES

Install the Shelf and Backplane Cable 1-1

Install Cards and Fiber-Optic Cable 2-1

Connect the PC and Log into the GUI 3-1

Turn Up Node 4-1

Add and Remove Nodes 14-1

Maintain the Node 15-1

Power Down the ONS 15454 16-1

Network Element Defaults C-1

Install the Shelf and Backplane Cable 1-1

Install Cards and Fiber-Optic Cable 2-1

Create Circuits and VT Tunnels 6-1

Manage Alarms 7-1

Monitor Performance 8-1

About this Manual

This guide explains how to install, turn up, provision, and maintain a Cisco ONS 15454 node and network.

The *Cisco ONS 15454 Troubleshooting Guide, Release 3.4* provides alarm clearing, general troubleshooting, and hardware replacement procedures.

To understand the procedures in context, such as their detailed purpose and process, refer to the *Cisco ONS 15454 Reference Manual, Release 3.4*.

Document Organization

This guide provides procedures for installation, turn up, provisioning and acceptance of ONS 15454 nodes and ONS 15454 designed networks. It is organized in a Cisco recommended work flow sequence for new installations, in addition to allowing easy access to procedures and tasks associated with adds, moves, and changes for existing installations.

Verification procedures are provided, where necessary, to allow contract vendors to complete the physical installation and then turn the site over to craft personnel for verification, provisioning, turn up and acceptance. The front matter of the book is present 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).

Non-Trouble Procedure (NTP)

Each NTP is a list of steps designed to accomplish a specific task. Follow the steps until the task is complete. For a crafts person requiring more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

Note To ensure that users who are not familiar with NTP and DLP acronyms understand the hierarchy within the guide, Uncaps are termed "procedures" and Depths 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 the crafts person through completion of a task. Some steps require that equipment indications be checked for verification. When the proper response is not obtained, a trouble clearing reference is provided.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

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

Ordering Documentation

You can order Cisco documentation in these ways:

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

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

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

CHAPTER 1

Install the Shelf and Backplane Cable

This chapter provides procedures for installing the Cisco ONS 15454. To view 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-1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4—Complete this procedure before continuing with the "NTP-2 Install the Shelf Assembly" procedure on page 1-5.
2. NTP-2 Install the Shelf Assembly, page 1-5—Complete this procedure to install the shelf assembly in a rack.
3. NTP-3 Open and Remove the Front Door, page 1-12—Complete this procedure to access the equipment before continuing with other procedures in this chapter.
4. NTP-4 Remove the Backplane Covers, page 1-15—Complete this procedure to access the backplane before continuing with other procedures in this chapter.
5. NTP-5 Install the Electrical Interface Assemblies, page 1-17—Complete this procedure if you plan to install electrical cards. This procedure is a prerequisite to the "NTP-9 Install the Electrical Card Cables on the Backplane" procedure on page 1-47.
6. NTP-6 Install the Power and Ground, page 1-23—Complete this procedure before continuing with the "NTP-7 Install the Fan-Tray Assembly" procedure on page 1-29.
7. NTP-7 Install the Fan-Tray Assembly, page 1-29—Complete this procedure to install the fan-tray assembly in the shelf.
8. NTP-119 Install the Alarm Expansion Panel, page 1-31—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.
9. NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-35—Complete this procedure to set up wire-wrap pin connections.
10. NTP-120 Install an External Wire-Wrap Panel to the AEP, page 1-42—Complete this procedure to connect an external wire-wrap panel to the AEP.
11. NTP-9 Install the Electrical Card Cables on the Backplane, page 1-47—Complete this procedure if you plan to install electrical cards.
12. NTP-10 Route Electrical Cables, page 1-55—Complete this procedure before continuing with the "NTP-11 Install the Rear Cover" procedure on page 1-57.

13. NTP-11 Install the Rear Cover, page 1-57—Complete this procedure to install the rear cover.
14. NTP-12 Install Ferrites, page 1-59—Complete this procedure to attach ferrites to power cables.
15. NTP-13 Perform the Shelf Installation Acceptance Test, page 1-61—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 non-combustible surfaces only.**

Required Tools and Equipment

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

Included 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)

User-Supplied Materials

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

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- 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, the #12 to #14 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 #14 AWG ground cable is required.

- Alarm cable pairs for all alarm connections, #22 or #24 AWG, solid tinned
- Shielded Building Integrated Timing Supply (BITS) clock cable pair #22 or #24, solid tinned
- 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 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-1 Unpack and Inspect the ONS 15454 Shelf Assembly

Purpose	This procedure describes how to unpack the ONS 15454 and verify the contents.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite

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

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

Step 3 Continue with the "NTP-2 Install the Shelf Assembly" procedure on page 1-5.

DLP-1 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

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 "Included Materials" section on page 1-2.

Note The fan-tray assembly is shipped separately.

Step 5 Return to your originating procedure (NTP).

DLP-2 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-1 Unpack and Verify the Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Open the shelf using the pinned hex key. For more information, see the "DLP-8 Open the Front Cabinet Compartment (Door)" task on page 1-12.

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-2 Install the Shelf Assembly

Purpose	This procedure describes how to reverse 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-1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite

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 3 inches (7.6 cm) of clearance around the ventilation openings.**

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.

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.**

Step 1 Complete the "DLP-3 Reverse the Mounting Bracket to Fit a 19-inch Rack" task on page 1-6 if you need to convert from a 23-inch to a 19-inch rack.

Step 2 To install the air filter in an alternative location, complete the "DLP-4 Install the External Brackets and Air Filter" task on page 1-7.

Step 3 Complete the necessary rack mount task:

- DLP-5 Mount the Shelf Assembly in a Rack (One Person), page 1-9
- DLP-6 Mount the Shelf Assembly in a Rack (Two People), page 1-10
- DLP-7 Mount Multiple Shelf Assemblies in a Rack, page 1-11

Step 4 Continue with the "NTP-3 Open and Remove the Front Door" procedure on page 1-12.

DLP-3 Reverse the Mounting Bracket to Fit a 19-inch Rack

Purpose	This task installs the mounting bracket to convert a 23-inch rack to a 19-inch 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

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 non-conductive 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).

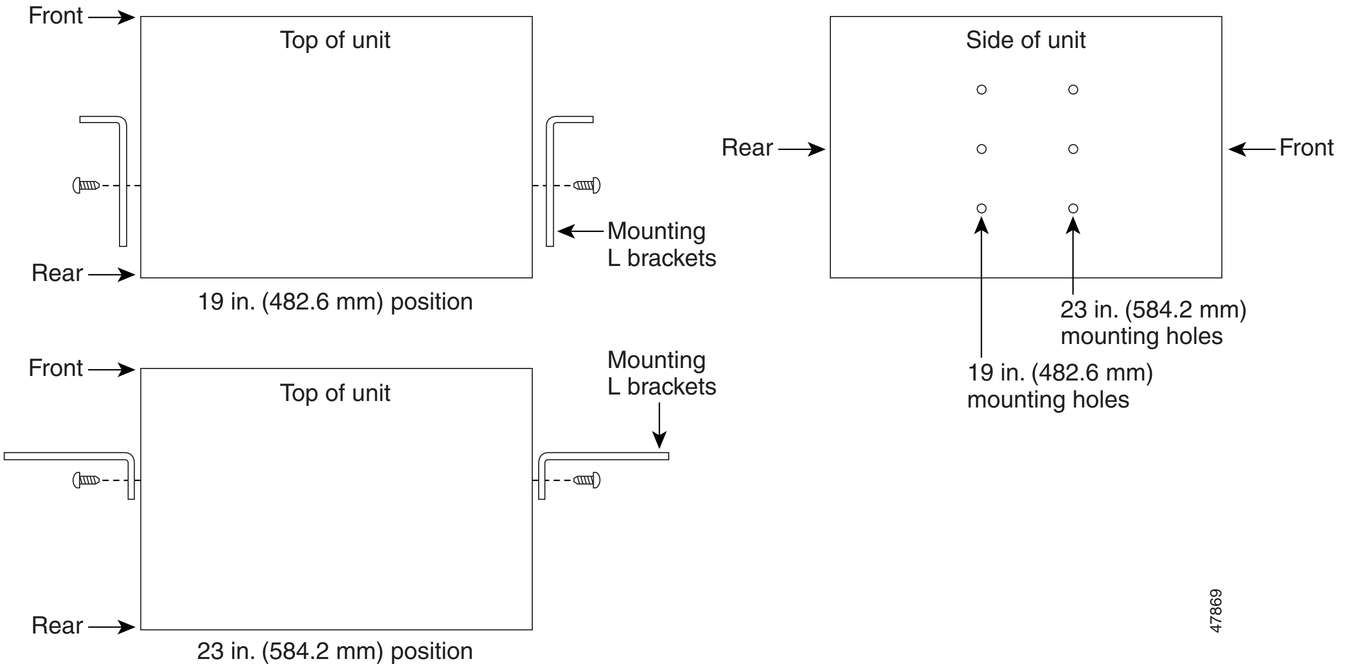
The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.

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 position to 19-inch position)



Step 7 Return to your originating procedure (NTP).

DLP-4 Install the External Brackets and Air Filter

The shelf assembly ships with external (bottom) brackets that you can use to install the air filter on the bottom of the shelf rather than beneath the fan-tray assembly. The brackets consist of two grooved metal pieces that attach to the bottom of the shelf assembly using three screws each. When you use the brackets to install the fan-tray air filter, you do not need to remove the fan-tray assembly to access the air filter. Attach the brackets to the bottom of the shelf assembly before installing the rack.

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.

Purpose	This task installs the external brackets and air filter.
Tools/Equipment	#2 Phillips screwdriver Medium slot head screwdriver Small slot head screwdriver
Prerequisite Procedures	DLP-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable
Required/As Needed	As needed; perform this task if you want to access the air filter without removing the fan-tray assembly.
Onsite/Remote	Onsite

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.

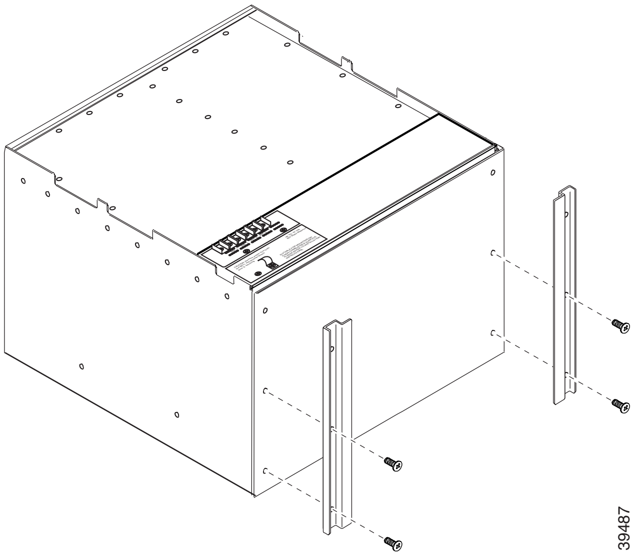
Step 2 Locate the three screw holes that run along the left and right sides of the bottom of the shelf assembly.

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 on page 1-8 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-5 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-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite

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

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

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-6 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-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite

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

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

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-7 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-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable • DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite

Note The ONS 15454 must have one inch 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 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 shelf assembly, a 100-amp fuse panel (30-amp fuse per shelf minimum) is required.
- If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-amp fuse panel (20-amp fuse per shelf minimum) is required.

Step 2 Mount the first ONS 15454 directly below the fuse and alarm panel using the "DLP-5 Mount the Shelf Assembly in a Rack (One Person)" task on page 1-9 or the "DLP-6 Mount the Shelf Assembly in a Rack (Two People)" task on page 1-10.

Step 3 Repeat the task with the second and third (fourth if applicable) ONS 15454s.

Step 4 Return to your originating procedure (NTP).

NTP-3 Open and Remove the Front Door

Purpose	This procedure describes how to open and remove the front door to access the equipment.
Tools/Equipment	Open end wrench Pinned hex key
Prerequisite Procedures	NTP-2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Complete the "DLP-8 Open the Front Cabinet Compartment (Door)" task on page 1-12.

Step 2 Complete the "DLP-9 Remove the Front Door" task on page 1-13.

Step 3 Continue with the "NTP-4 Remove the Backplane Covers" procedure on page 1-15.

DLP-8 Open the Front Cabinet Compartment (Door)

Purpose	This task opens the front cabinet compartment door.
Tools/Equipment	Pinned hex key
Prerequisite Procedures	DLP-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable DLP-5 Mount the Shelf Assembly in a Rack (One Person), page 1-9 or DLP-6 Mount the Shelf Assembly in a Rack (Two People), page 1-10 DLP-7 Mount Multiple Shelf Assemblies in a Rack, page 1-11, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite

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.

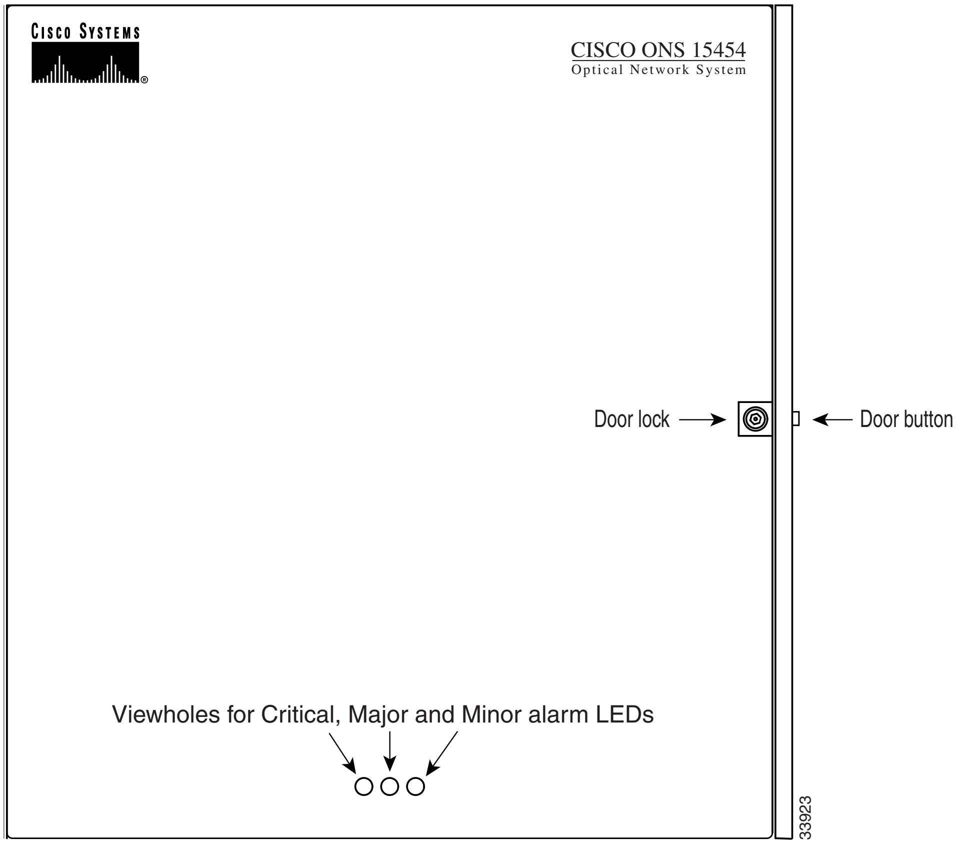
Step 1 Open the front door lock (Figure 1-3 on page 1-13).

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 The ONS 15454 front door



Step 4 Return to your originating procedure (NTP).

DLP-9 Remove the Front Door

Purpose	This task removes the front cabinet compartment door.
Tools/Equipment	Open end wrench
Prerequisite Procedures	DLP-8 Open the Front Cabinet Compartment (Door), page 1-12
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Open the door.

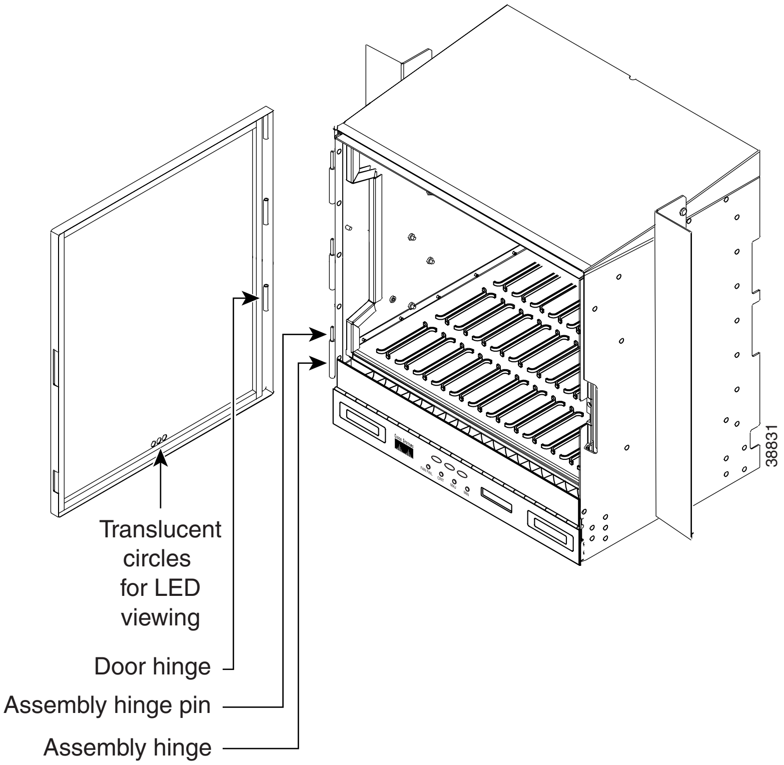
Step 2 To remove the door ground strap (available in Release 3.3 and later), perform the following:

a. To detach the ground strap from the front door, loosen the #6 Kepnut (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 Kepnut (49-0337-01) on the terminal lug using the open end wrench. Remove the terminal lug and lock washer.

Step 3 Lift the door from its hinges at the top left-hand corner of the door (Figure 1-4).

Figure 1-4 Removing the ONS 15454 front door



Step 4 Return to your originating procedure (NTP).

NTP-4 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-2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Complete the "DLP-10 Remove the Lower Backplane Cover" task on page 1-15.

Step 2 Complete the "DLP-11 Remove the Backplane Sheet Metal Cover" task on page 1-16.

Step 3 If you plan to install Electrical Interface Assemblies (EIAs), continue with the "NTP-5 Install the Electrical Interface Assemblies" procedure on page 1-17. If not, continue with the "NTP-6 Install the Power and Ground" procedure on page 1-23.

DLP-10 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	• DLP-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable • DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable • DLP-5 Mount the Shelf Assembly in a Rack (One Person), page 1-9 or DLP-6 Mount the Shelf Assembly in a Rack (Two People), page 1-10 • DLP-7 Mount Multiple Shelf Assemblies in a Rack, page 1-11, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite

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-11 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-3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable DLP-4 Install the External Brackets and Air Filter, page 1-7, if applicable DLP-5 Mount the Shelf Assembly in a Rack (One Person), page 1-9 or DLP-6 Mount the Shelf Assembly in a Rack (Two People), page 1-10 DLP-7 Mount Multiple Shelf Assemblies in a Rack, page 1-11, if applicable
Required/As Needed	Required
Onsite/Remote	Onsite

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-5 Install the Electrical Interface Assemblies

Purpose	This procedure describes how to install electrical interface assemblies (EIAs). Typically an EIA panel is already installed on the backplane when the node is received, 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 9 perimeter screws 12 inner screws 5 backplane cover screws EIA card (SMB, BNC, AMP Champ) EIA panel
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required if the node will use electrical signals
Onsite/Remote	Onsite

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.

Step 1 Complete the "DLP-12 Install a BNC or High-Density BNC EIA" task on page 1-18 as needed. BNCs are locking connectors; the high-density BNC also allows you to access every port on every card.

Step 2 Complete the "DLP-13 Install an SMB EIA" task on page 1-20 as needed. SMBs allow you to access every port on every card using more space and efficient cabling.

Step 3 Complete the "DLP-14 Install the AMP Champ EIA" task on page 1-21 as needed. AMP champs are exclusive to DS-1 cables.

Note To attach cables to the EIAs, see the "NTP-9 Install the Electrical Card Cables on the Backplane" procedure on page 1-47.

Step 4 Continue with the "NTP-6 Install the Power and Ground" procedure on page 1-23.

DLP-12 Install a BNC or High-Density BNC EIA

Purpose	This task installs a BNC or high-density BNC EIA.
Tools/Equipment	#2 Phillips screwdriver Medium slot head screwdriver Small slot head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws BNC or high-density BNC card EIA cover
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer a BNC interface to an SMB interface
Onsite/Remote	Onsite

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 8-10 lbs 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 8-10 lbs to secure the cover panel to the card and backplane.

Figure 1-5 on page 1-19 shows a BNC EIA installation. Figure 1-6 on page 1-19 shows high-density BNC EIA installation.

Figure 1-5 Installing the BNC EIA

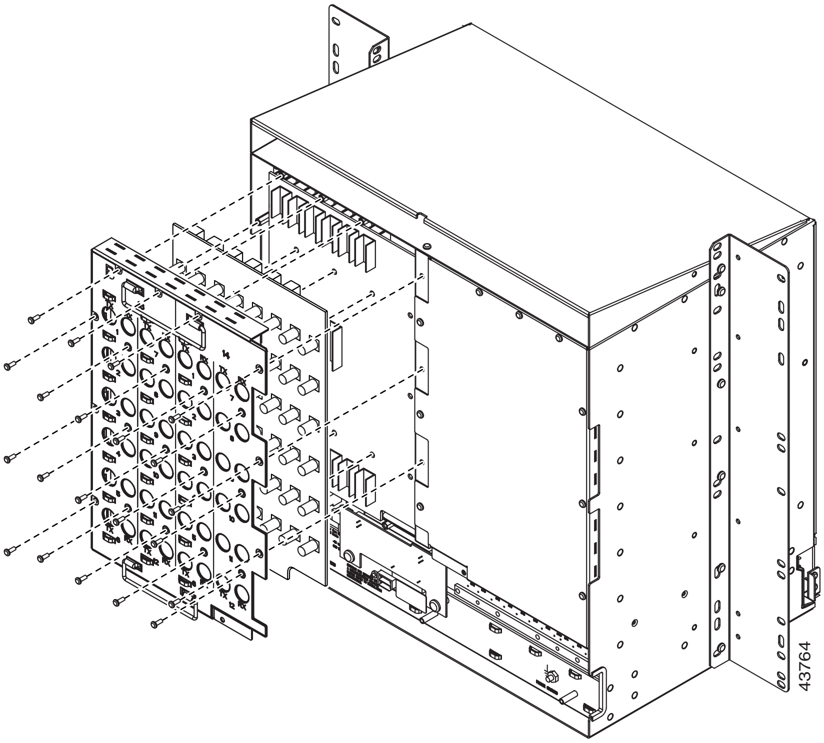
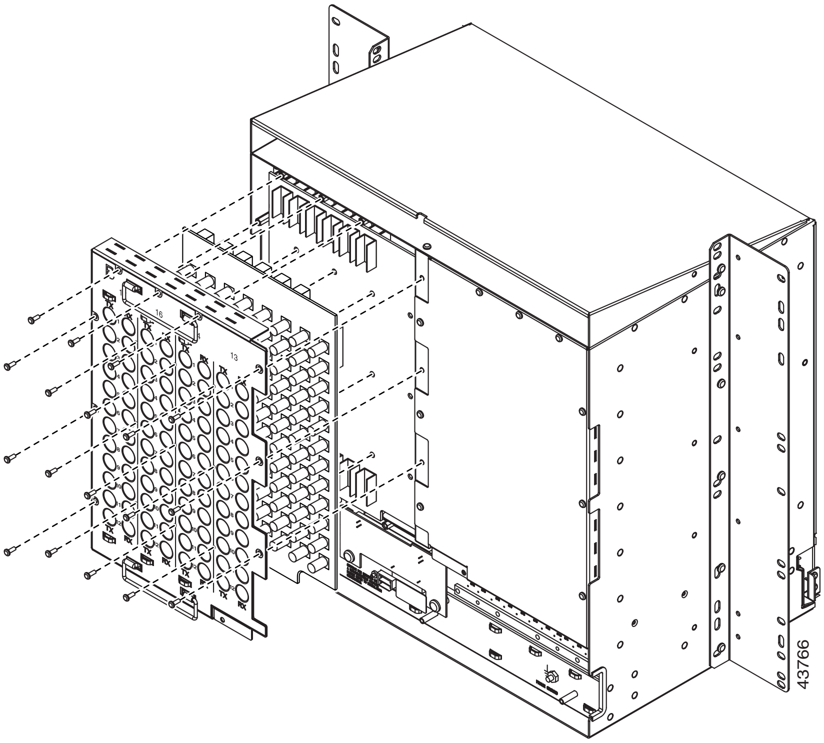


Figure 1-6 Installing the high-density BNC EIA



Step 5 Return to your originating procedure (NTP).

DLP-13 Install an SMB EIA

Purpose	This task installs an SMB EIA.
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	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required 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
Onsite/Remote	Onsite

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 8-10 lbs to secure the cover panel to the backplane.

Step 4 Insert and tighten the twelve inner screws (P/N 48-0004) at 8-10 lbs 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=).

Step 5 Return to your originating procedure (NTP).

DLP-14 Install the AMP Champ EIA

Purpose	This task installs an AMP Champ EIA.
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	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required if you are using DS1-14 cards and prefer an AMP interface to an SMB interface
Onsite/Remote	Onsite

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

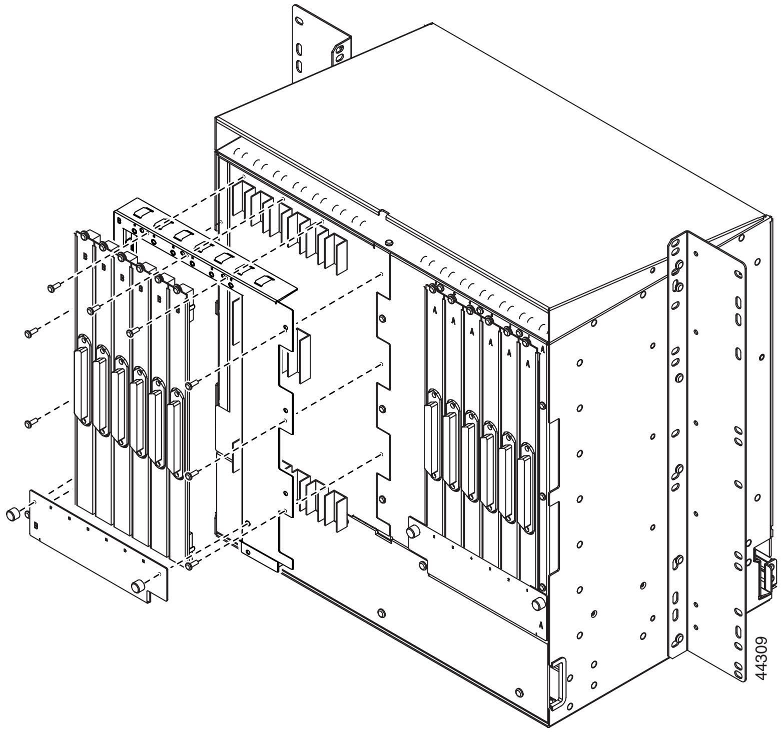
Step 2 Align an AMP Champ card with the backplane connector and push until it fits snugly. Repeat until you have installed all six AMP Champ cards.

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 8-10 lbs.

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

Figure 1-7 shows an AMP Champ EIA installation.

Figure 1-7 Installing the AMP Champ EIA



Step 5 Return to your originating procedure (NTP).

NTP-6 Install the Power and Ground

Purpose	This procedure describes how to install 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-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required
Onsite/Remote	Onsite

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.**

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.

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.**

Step 1 Complete the "DLP-15 Verify that the Correct Fuse and Alarm Panel is Installed in the Equipment Rack" task on page 1-24.

Step 2 Complete the "DLP-16 Connect the Office Ground to the ONS 15454" task on page 1-25.

Step 3 Complete the "DLP-17 Connect Office Power to the ONS 15454 Shelf" task on page 1-26.

Step 4 Complete the "DLP-18 Turn On and Verify Office Power" task on page 1-28.

Step 5 Continue with the "NTP-7 Install the Fan-Tray Assembly" procedure on page 1-29.

DLP-15 Verify that the Correct Fuse and Alarm Panel is Installed in the Equipment Rack

Purpose	This task verifies that the proper fuse and alarm panel is installed in the equipment rack.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Verify the following:

- If using the 15454-SA-ANSI shelf, a 100-amp fuse panel (30-amp fuse per shelf minimum) is installed. If not, install one according to manufacturer's instructions.
- If using the 15454-SA-NEBS3 shelf, a standard 80-amp fuse panel (20-amp fuse per shelf minimum) is installed. If not, install one according to manufacturer's instructions.

Step 2 Return to your originating procedure (NTP).

DLP-16 Connect the Office Ground to the ONS 15454

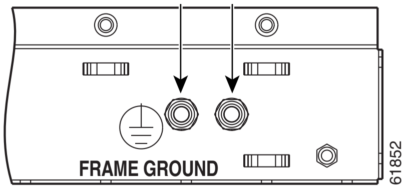
Purpose	This task connects ground to the ONS 15454 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot head screwdriver Small slot head screwdriver Screws Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors
Prerequisite Procedures	DLP-10 Remove the Lower Backplane Cover, page 1-15
Required/As Needed	Required
Onsite/Remote	Onsite

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 (#6 AWG) to the right side of the backplane ground nut. See Figure 1-8 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-lbs. 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 1-8 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-17 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-15 Verify that the Correct Fuse and Alarm Panel is Installed in the Equipment Rack, page 1-24 DLP-16 Connect the Office Ground to the ONS 15454, page 1-25
Required/As Needed	Required
Onsite/Remote	Onsite

Note If the system loses power or both TCC+ cards are reset and the system is not provisioned to get the time from an 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-25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-3.

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

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.**

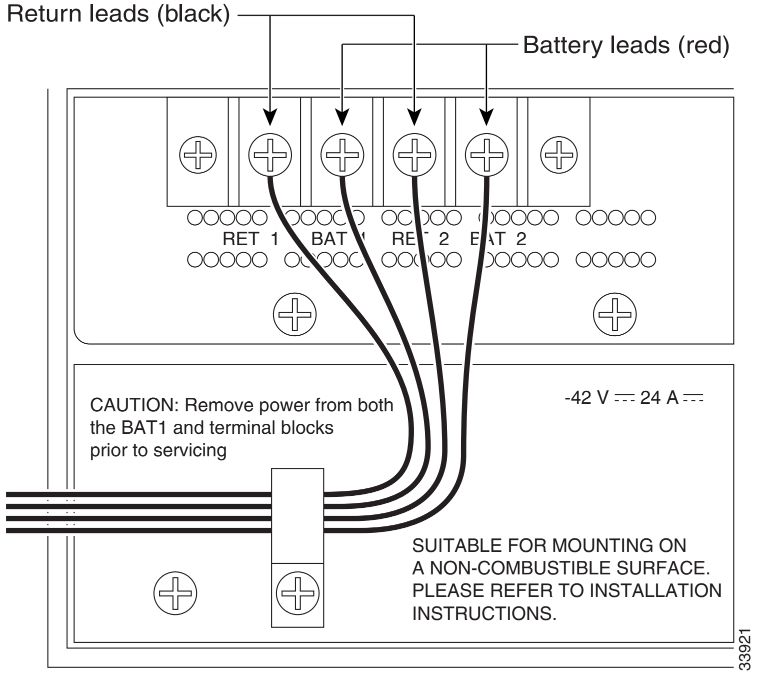
Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15454 from the fuse panel. Figure 1-9 on page 1-27 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 1-9 ONS 15454 power terminals


Return leads (black)
Battery leads (red)
RET 1
BAT 1
RET 2
BAT 2
CAUTION: Remove power from both the BAT1 and terminal blocks prior to servicing
-42 V ⎓ 24 A ⎓
SUITABLE FOR MOUNTING ON A NON-COMBUSTIBLE SURFACE. PLEASE REFER TO INSTALLATION INSTRUCTIONS.
33921

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 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 1-9 on page 1-27, follow a torque specification of 10 in-lbs.

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

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 non-corrosive.

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 non-corrosive.

Step 10 Route the cables out below the power terminals using the plastic cable clamp, as shown in Figure 1-9 on page 1-27.

Step 11 Return to your originating procedure (NTP).

DLP-18 Turn On and Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-15 Verify that the Correct Fuse and Alarm Panel is Installed in the Equipment Rack, page 1-24 DLP-16 Connect the Office Ground to the ONS 15454, page 1-25 DLP-17 Connect Office Power to the ONS 15454 Shelf, page 1-26
Required/As Needed	Required
Onsite/Remote	Onsite

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 -42 VDC and -57 VDC. Place the red test lead on the B-side connection and verify that it is between -42 VDC and -57 VDC.

Note The voltages -42 VDC and -57 VDC are, respectively, the minimum and maximum amperages 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-amp fuse panel, insert a 20-amp fuse into the fuse position according to site practice.
- If you are using a 100-amp fuse panel, insert a 30-amp 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 it reads between -42 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 -42 VDC and -57 VDC are, respectively, the minimum and maximum amperages 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 it reads between -42 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-7 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-3 Open and Remove the Front Door, page 1-12 NTP-6 Install the Power and Ground, page 1-23
Required/As Needed	Required
Onsite/Remote	Onsite

Caution Do not operate an ONS 15454 without a fan-tray air filter. A fan-tray air filter is mandatory.

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). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N 800-0714915454). Installing the 15454-FTA3 in a non-compliant shelf assembly may 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.

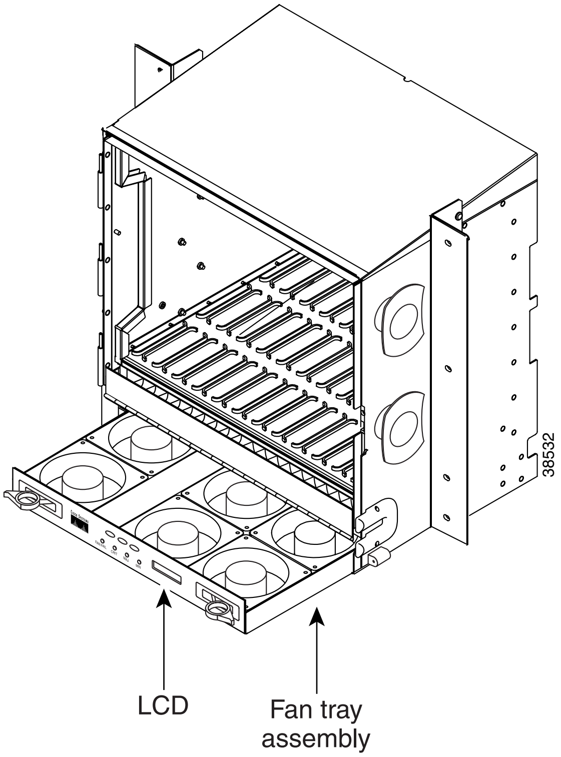
Note To install the fan-tray assembly, it is not necessary to move any of the cable-management facilities.

Step 1 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 2 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated and displays data.

Figure 1-10 shows the location of the fan tray.

Figure 1-10 Installing the fan-tray assembly



Step 3 Continue with the "NTP-119 Install the Alarm Expansion Panel" procedure on page 1-31 if you plan to install an Alarm Expansion Panel (AEP). If not, continue with the "NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-35.

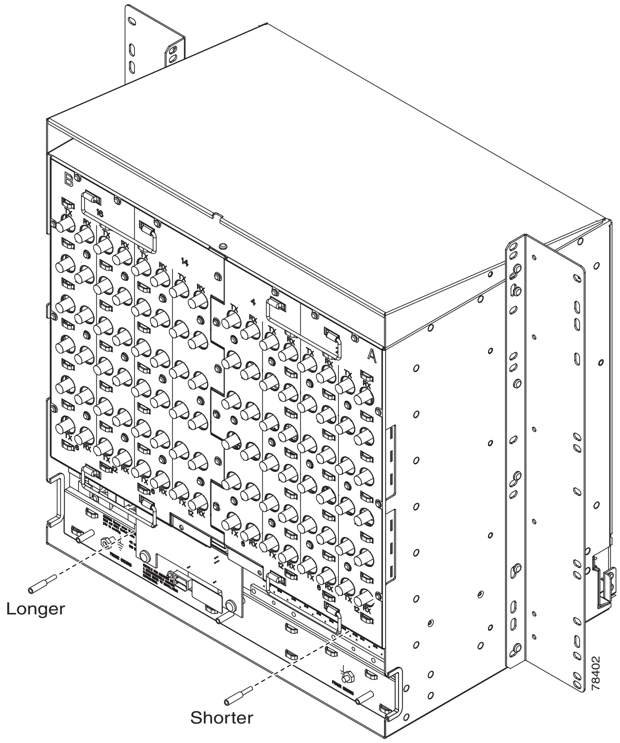
NTP-119 Install the Alarm Expansion Panel

Purpose	This procedure installs an Alarm Expansion Panel (AEP) onto the 15454-SA-ANSI shelf backplane that 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.
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-10 Remove the Lower Backplane Cover, page 1-15
Required/As Needed	Required if you are terminating more than 16 alarm contacts (16 inputs + 0 outputs or 12 inputs or 4 outputs); the AIC-I card must be installed before you can provision the alarm contacts enabled by the AEP.
Onsite/Remote	Onsite

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 1-11 on page 1-32).

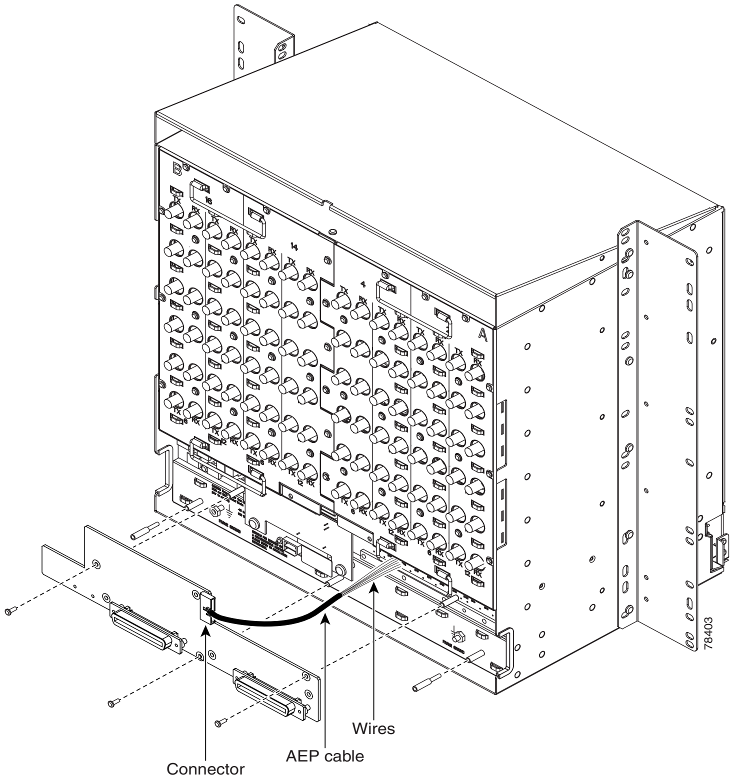
Figure 1-11 Replace backplane screws with standoffs



Step 2 Attach the remaining two standoffs on either side of the backplane (Figure 1-12 on page 1-33).

Step 3 Position the AEP board over the standoffs (Figure 1-12 on page 1-33).

Figure 1-12 Installing standoffs and the AEP



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

Step 5 Attach the open ends of the wires from the AEP board to the wire-wrap pins on the backplane of the shelf (Figure 1-13 on page 1-34). Table 1-1 on page 1-34 lists the AEP pin assignments.

Figure 1-13 AEP wire-wrap connections to backplane pins

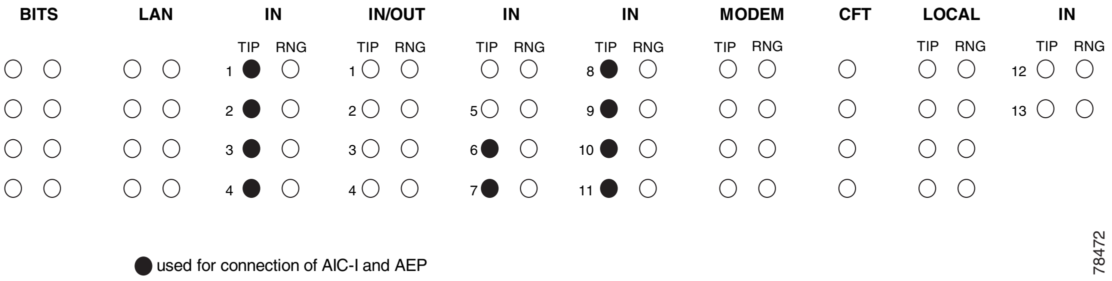


Table 1-1 Pin Assignments for the AEP

Wire	Pin	AEP signal	AIC-I signal
Tip 1	7	AEP_GND	GND
Tip 2	8	AEP_+5	AE_+5
Tip 3	9	VBAT-	VBAT-
Tip 4	10	VB+	VB+
Tip 6	6	AE_CLK_P	AE_CLK_P
Tip 7	5	AE_CLK_N	AE_CLK_N
Tip 8	4	AE_DOUT_P	AE_DIN_P
Tip 9	3	AE_DOUT_N	AE_DIN_N
Tip 10	2	AE_DIN_P	AE_DOUT_P
Tip 11	1	AE_DIN_N	AE_DOUT_N

Step 6 Attach the connector on the opposite end of the cable assembly to the RS-485 connector port on the AEP (Figure 1-12 on page 1-33).

Step 7 Continue with the "NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-35.

NTP-8 Install 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 alarm wires
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	As needed
Onsite/Remote	Onsite

Step 1 Complete the "DLP-19 Install Alarm Wires on the Backplane" task on page 1-36 as necessary (if you are using an AIC or AIC-I card and not using an AEP).

Step 2 Complete the "DLP-20 Install Timing Wires on the Backplane" task on page 1-39 as needed. Timing wires are necessary to provision external timing.

Step 3 Complete the "DLP-21 Install LAN Wires on the Backplane" task on page 1-40 as needed. LAN wires (or the LAN port on the TCC+) are necessary to create an external LAN connection.

Step 4 Complete the "DLP-22 Install the TL1 Craft Interface" task on page 1-41 as needed. Craft wires (or the RS-232 port on the TCC+) 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-120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-42.
- If you did not install an AEP and you plan to install electrical cards, continue with the "NTP-9 Install the Electrical Card Cables on the Backplane" procedure on page 1-47.
- If you did not install an AEP and do not plan to install electrical cards, continue with the "NTP-11 Install the Rear Cover" procedure on page 1-57.

DLP-19 Install Alarm Wires on the Backplane

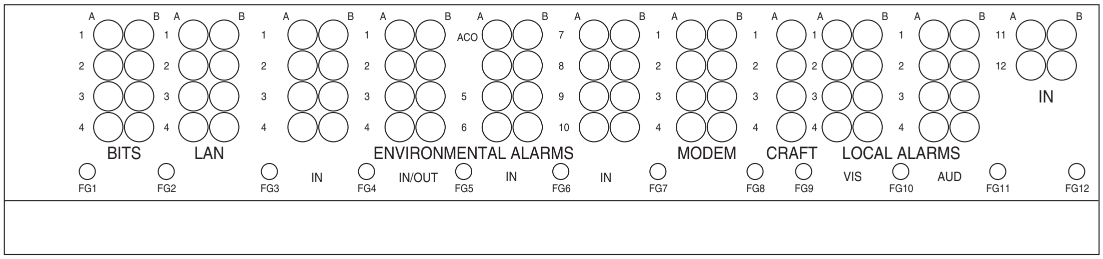
Purpose	This task installs alarm wires on the backplane so that you can provision external (environmental) alarms and controls with the AIC or AIC-I card. If you are using the AEP, do not perform this task.
Tools/Equipment	Wire wrapper #22 or #24 AWG wires
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required to create external alarms and controls without the AEP
Onsite/Remote	Onsite

Step 1 Use #22 or #24 AWG wires.

Step 2 Wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Figure 1-14 shows alarm pin assignments for the Release 3.4 ONS 15454 backplane. Figure 1-15 on page 1-38 shows alarm pin assignments for the backplane used for Release 3.3 and earlier.

For information about attaching ferrites to wire-wrap pin fields, see the "NTP-12 Install Ferrites" section on page 1-59.

Figure 1-14 ONS 15454 backplane pinouts (Release 3.4)



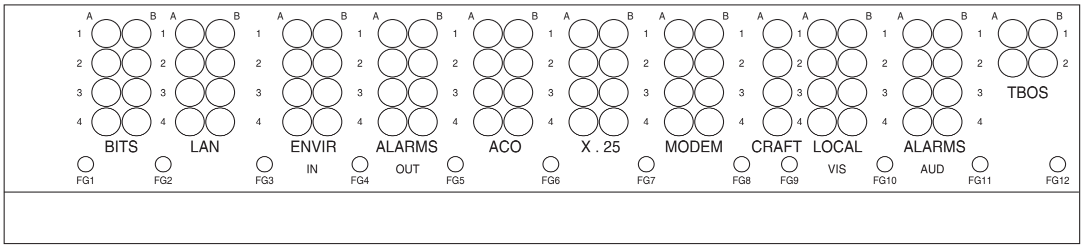
Field	Pin	Function
BITS	A1	BITS Output 2 negative (–)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (–)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (–)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (–)
	B4	BITS Input 1 positive (+)
LAN	Connecting to a hub, or switch	
	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 1-15 ONS 15454 backplane pinouts (Release 3.3 and 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.

Step 3 Return to your originating procedure (NTP).

DLP-20 Install Timing Wires on the Backplane

Purpose	This task installs the timing wires on the backplane.
Tools/Equipment	Wire wrapper #22 or #24 AWG wire
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required if the node is using external BITS timing
Onsite/Remote	Onsite

Step 1 Use #22 or #24 AWG wire.

Step 2 Wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

The BITS pin field (FG1) has a frame ground pin beneath it. Wrap the ground shield of the alarm cable to the frame ground pin. Table 1-2 lists the pin assignments for the BITS timing pin fields.

Table 1-2 External Timing Pin Assignments for BITS

External Device	Contact	Tip & Ring	Function
First external device	A3 (BITS 1 Out)	Primary ring (-)	Output to external device
	B3 (BITS 1 Out)	Primary tip (+)	Output to external device
	A4 (BITS 1 In)	Secondary ring (-)	Input from external device
	B4 (BITS 1 In)	Secondary tip (+)	Input from external device
Second external device	A1 (BITS 2 Out)	Primary ring (-)	Output to external device
	B1 (BITS 2 Out)	Primary tip (+)	Output to external device
	A2 (BITS 2 In)	Secondary ring (-)	Input from external device
	B2 (BITS 2 In	Secondary tip (+)	Input from external device

Note For more detailed information about timing, refer to the *Cisco ONS 15454 Reference Manual.* To set up system timing, see the "NTP-28 Set Up Timing" procedure on page 4-18.

Step 3 Return to your originating procedure (NTP).

DLP-21 Install LAN Wires on the Backplane

Purpose	This task installs the LAN wires on the backplane.
Tools/Equipment	Wire wrapper #22 or #24 AWG wire
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required if the node is using an external LAN connection
Onsite/Remote	Onsite

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

Step 1 Use #22 or #24 AWG wire.

Step 2 Wrap the wires on the appropriate wire-wrap pins according to local site practice.

Caution Cross talk may result if both Rx and Tx pins connect on the same twisted pair of wires from the CAT 5 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
LAN 1 Connecting to data circuit-terminating equipment (DCE*) (a hub or switch)	B2	1
	A2	2
	B1	3
	A1	6
LAN 1 Connecting to data terminal equipment (DTE) (a PC/workstation or router)	B1	1
	A1	2
	B2	3
	A2	6

Step 3 Return to your originating procedure (NTP).

DLP-22 Install the TL1 Craft Interface

Purpose	This task installs the TL1 craft interface.
Tools/Equipment	Wire wrapper #22 or #24 AWG alarm wires
Prerequisite Procedures	NTP-4 Remove the Backplane Covers, page 1-15
Required/As Needed	Required to access TL1 using the craft backplane pins
Onsite/Remote	Onsite

Note Rather than using the craft pins, you can use a LAN cable connected to the TCC+ RS-232 port to access a TL1 craft interface.

Step 1 Use #22 or #24 AWG wire.

Step 2 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-31 Attach Ferrites to Wire-Wrap Pin Fields" task on page 1-60.

Step 3 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 RS-232 port on the TCC+ 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

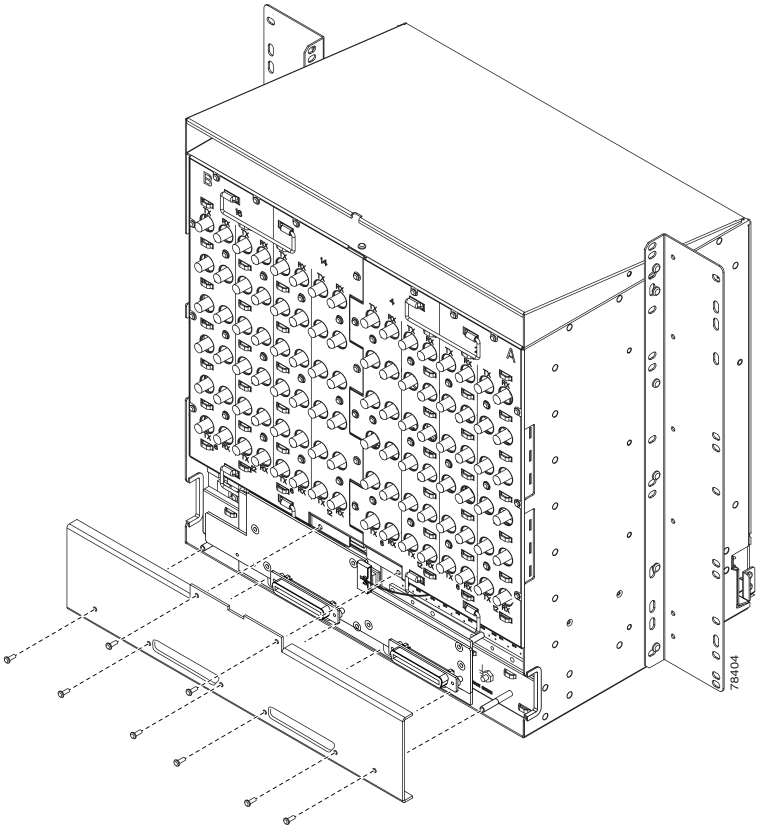
Step 4 Return to your originating procedure (NTP).

NTP-120 Install an External Wire-Wrap Panel to the AEP

Purpose	This procedure connects an external wire-wrap panel to the Alarm Expansion Panel (AEP) to provide the physical alarm contacts for the AEP.
Tools/Equipment	External wire-wrap panel
Prerequisite Procedures	NTP-119 Install the Alarm Expansion Panel, page 1-31
Required/As Needed	Required if you installed an AEP
Onsite/Remote	Onsite

Step 1 Position the lower cover over the AEP. Make sure that the AEP AMP Champ connectors protrude through the cut-outs in the lower cover (Figure 1-16 on page 1-42).

Figure 1-16 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 1-6 lists the alarm output pin assignments. Figure 1-17 and Figure 1-18 illustrate the alarm input and output connectors, respectively.

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-
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	N.C.
25	ALARM_IN_+	51	GND1
26	ALARM_IN_0-	52	GND2

Table 1-6 Alarm Output Pin Assignments

AMP Champ Pin	Signal name	AMP Champ Pin	Signal name
1	N.C.	27	COM_0
2	COM_1	28	N.C.
3	NO_1	29	NO_2
4	N.C.	30	COM_2
5	COM_3	31	N.C.
6	NO_3	32	NO_4

Table 1-6 Alarm Output Pin Assignments (continued)

AMP Champ Pin	Signal name	AMP Champ Pin	Signal name
7	N.C.	33	COM_4
8	COM_5	34	N.C.
9	NO_5	35	NO_6
10	N.C.	36	COM_6
11	COM_7	37	N.C.
12	NO_7	38	NO_8
13	N.C.	39	COM_8
14	COM_9	40	N.C.
15	NO_9	41	NO_10
16	N.C.	42	COM_10
17	COM_11	43	N.C.
18	NO_11	44	NO_12
19	N.C.	45	COM_12
20	COM_13	46	N.C.
21	NO_13	47	NO_14
22	N.C.	48	COM_14
23	COM_15	49	N.C.
24	NO_15	50	N.C.
25	N.C.	51	GND1
26	NO_0	52	GND2

Figure 1-17 Alarm input connector

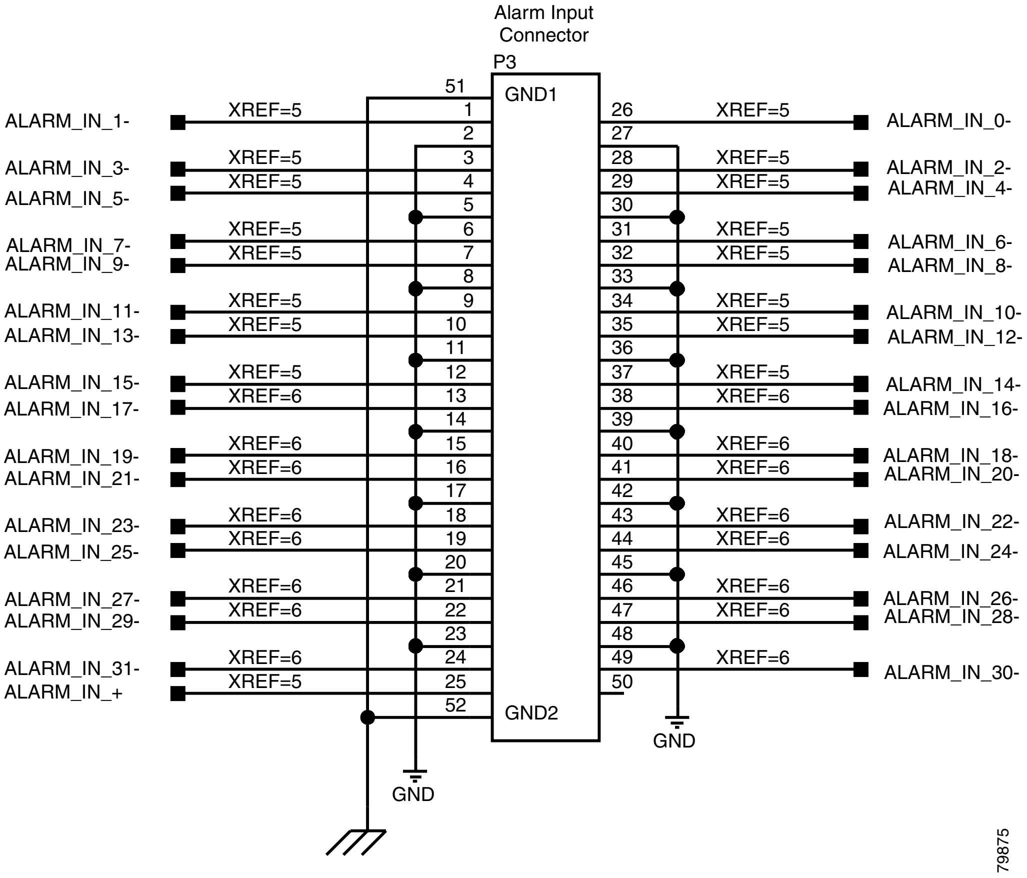
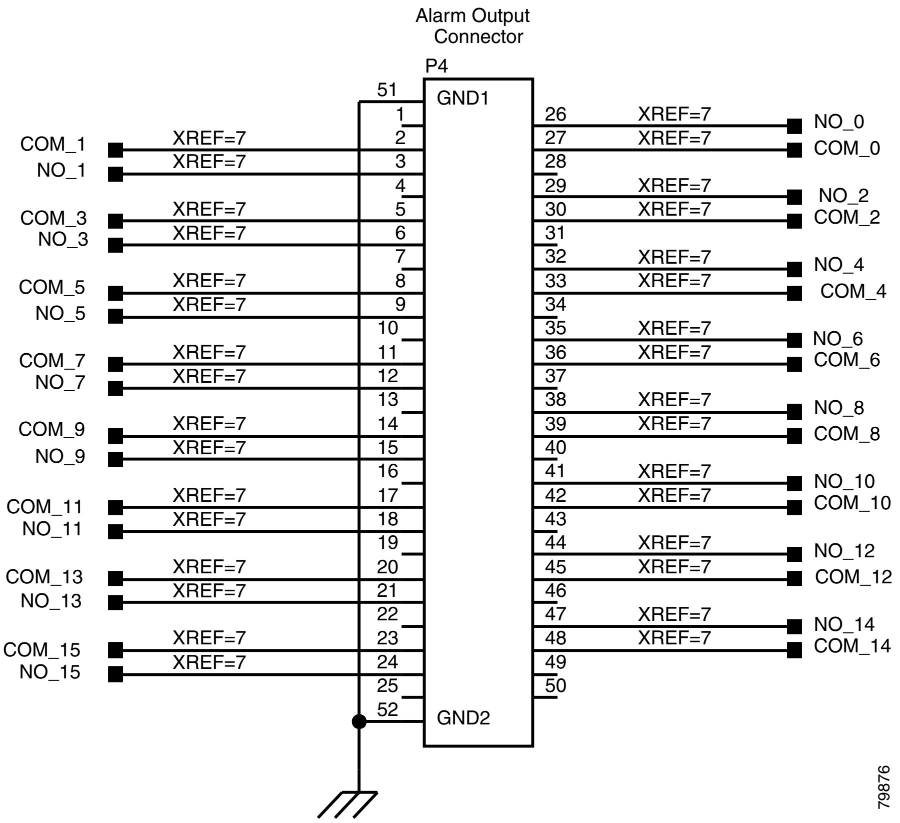


Figure 1-18 Alarm output connector



Step 4 Complete one of the following:

- If you plan to install electrical cards, continue with the "NTP-9 Install the Electrical Card Cables on the Backplane" procedure on page 1-47.
- If you do not plan to install electrical cards, continue with the "NTP-11 Install the Rear Cover" procedure on page 1-57.

NTP-9 Install the Electrical Card Cables on the Backplane

Purpose	Optional 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
Prerequisite Procedures	NTP-5 Install the Electrical Interface Assemblies, page 1-17
Required/As Needed	Required if you are using electrical cards
Onsite/Remote	Onsite

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-23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)" task on page 1-48 as needed. Baluns are used on SMB EIAs to properly terminate DS-1 signals.

Step 2 To install DS-1 cables using AMP Champ cables, complete the "DLP-24 Install DS-1 AMP Champ Cables on the AMP Champ EIA" task on page 1-49.

Step 3 Complete the "DLP-25 Install Coaxial Cable With BNC Connectors" task on page 1-52 as needed.

Step 4 Complete the "DLP-26 Install Coaxial Cable With High-Density BNC Connectors" task on page 1-53 as needed.

Step 5 Complete the "DLP-27 Install Coaxial Cable with SMB Connectors" task on page 1-54 as needed.

Step 6 Continue with the "NTP-10 Route Electrical Cables" procedure on page 1-55.

DLP-23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)

Purpose	This task installs the DS-1 cables using the electrical interface adapters.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-13 Install an SMB EIA, page 1-20
Required/As Needed	Required if you are using an SMB EIA for DS1N-14 cards
Onsite/Remote	Onsite

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 beyond the SMB EIA.

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.

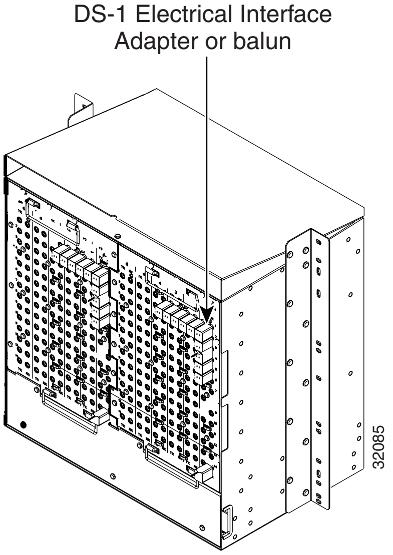
b. Connect the transmit cables to the transmit adapter pins on the backplane connector for the desired port.

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 1-19 on page 1-49 shows a ONS 15454 backplane with an SMB EIA with DS-1 electrical interface adapters attached on both sides of the shelf assembly to create DS-1 twisted-pair termination points.

Figure 1-19 A backplane with an SMB EIA for DS-1 cables



Step 4 Return to your originating procedure (NTP).

DLP-24 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-14 Install the AMP Champ EIA, page 1-21
Required/As Needed	Required if you are using an AMP Champ EIA for DS1N-14 cards
Onsite/Remote	Onsite

Step 1 Prepare a 56-wire cable for each 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 on page 1-50 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA. 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 (Shaded Area Corresponds to White/Orange Binder Group)

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 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

Table 1-8 on page 1-51 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).

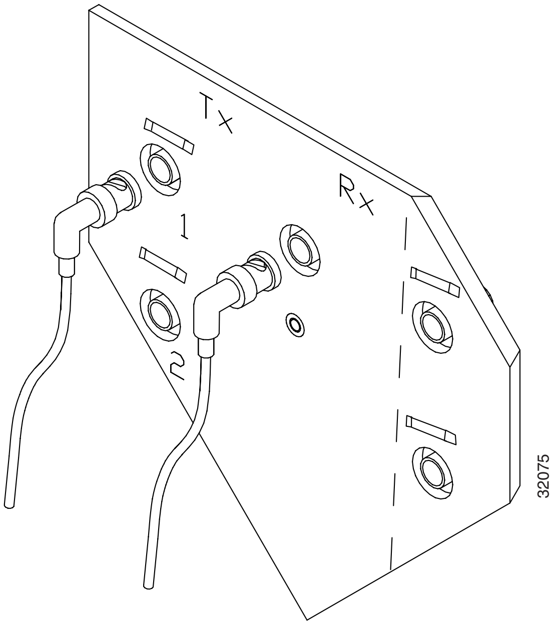
DLP-25 Install Coaxial Cable With BNC Connectors

Purpose	This task installs the coaxial cable with BNC connectors.
Tools/Equipment	None
Prerequisite Procedures	DLP-12 Install a BNC or High-Density BNC EIA, page 1-18
Required/As Needed	Required if you are using DS3-12, DS3XM-6, or EC-1 cards and are using a BNC interface rather than an SMB interface
Onsite/Remote	Onsite

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

Figure 1-20 shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

Figure 1-20 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-26 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-12 Install a BNC or High-Density BNC EIA, page 1-18
Required/As Needed	Required if you are using DS3-12, DS3XM-6, or EC-1 cards and are using a BNC interface rather than an SMB interface
Onsite/Remote	Onsite

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-27 Install Coaxial Cable with SMB Connectors

Purpose	This task installs the coaxial cable with SMB connectors. Refer to Figure 1-21 when performing task.
Tools/Equipment	SMB cable connector
Prerequisite Procedures	DLP-13 Install an SMB EIA, page 1-20
Required/As Needed	Required if you are using DS3-12, DS3XM-6, or EC-1 cards and are using an SMB interface rather than a BNC interface
Onsite/Remote	Onsite

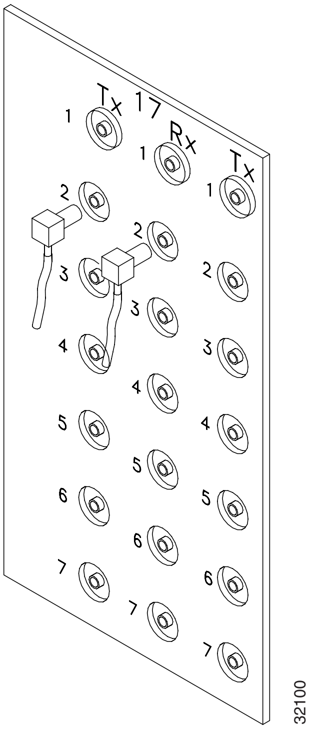
Step 1 Place the SMB cable connector over the desired connection point on the backplane.

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 1-21 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-10 Route Electrical Cables

Purpose	The following procedure explains how to route and manage electrical (backplane) cables.
Tools/Equipment	RG179, RG59 (735A) 26 AWG cable, or RG59 (734A) 20 AWG cable
Prerequisite Procedures	NTP-9 Install the Electrical Card Cables on the Backplane, page 1-47
Required/As Needed	Required if using electrical cards
Onsite/Remote	Onsite

Step 1 To route coaxial cables, complete the "DLP-28 Route Coaxial Cables" task on page 1-55.

Step 2 To route DS-1 twisted pair cables, complete the "DLP-29 Route DS-1 Twisted-Pair Cables" task on page 1-56.

Step 3 Continue with the "NTP-11 Install the Rear Cover" procedure on page 1-57.

DLP-28 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	DLP-25 Install Coaxial Cable With BNC Connectors, page 1-52 DLP-26 Install Coaxial Cable With High-Density BNC Connectors, page 1-53 DLP-27 Install Coaxial Cable with SMB Connectors, page 1-54
Required/As Needed	Required
Onsite/Remote	Onsite

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.

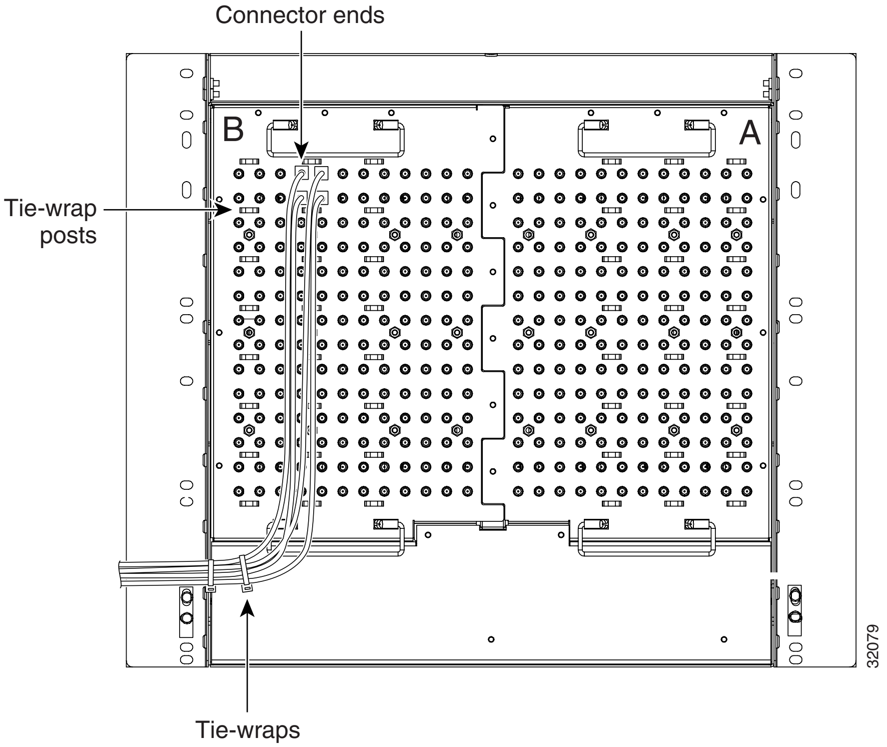
Step 3 Use standard RG59 (735A) cable connected to the RG179 for the remainder of the cable run. When using a 10-foot section of the RG179, you can attach a maximum length of 437 feet of RG59 (735A). When using a 30-foot section of RG179, you can attach a maximum length of 311 feet of RG59 (735A).

When using the RG179 cable, the maximum distance available (122 feet) is less than the maximum distance available with standard RG59 (735A) cable (306 feet). The maximum distance when using the RG59 (734A) cable is 450 feet. 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 @ 22 MHz.
- For RG59 (735A), the attenuation rate is 23 dB/kft @ 22 MHz.

Use a figure of 5.0 for total cable loss when making calculations. Figure 1-22 on page 1-56 shows an example of proper coaxial cable routing.

Figure 1-22 Routing coaxial cable (SMB EIA backplane)



Step 4 Return to your originating procedure (NTP).

DLP-29 Route DS-1 Twisted-Pair Cables

Purpose	This task routes the DS-1 twisted-pair cables.
Tools/Equipment	None
Prerequisite Procedures	DLP-23 Install DS-1 Cables Using Electrical Interface Adapters (Balun), page 1-48
Required/As Needed	Required
Onsite/Remote	Onsite

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.

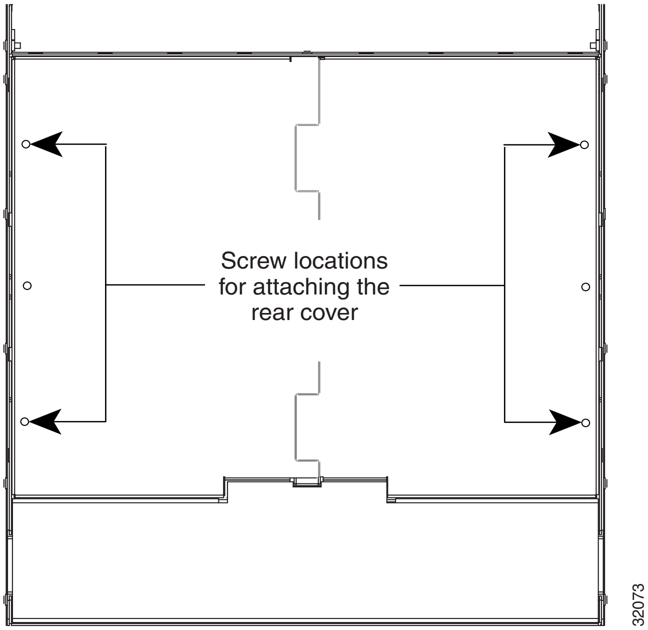
Step 3 Return to your originating procedure (NTP).

NTP-11 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	None
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Locate the three screws that run vertically along both edges of the backplane (Figure 1-23 on page 1-57).

Figure 1-23 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.

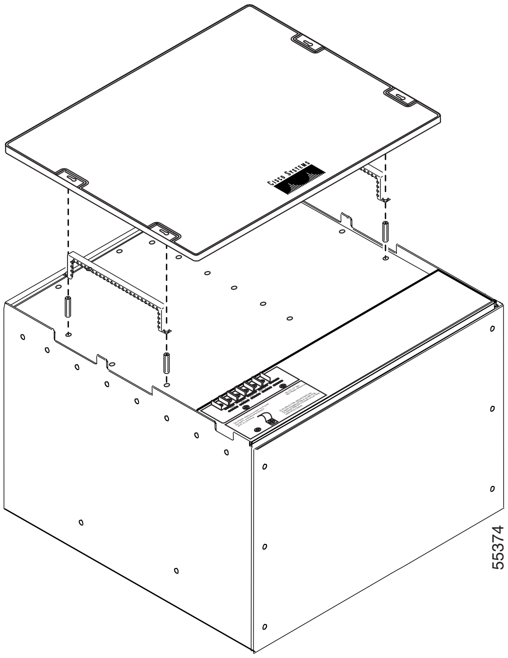
Step 3 Slide one of the mounting brackets into place and tighten the screws.

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 1-24 shows rear cover installation using spacers.

Figure 1-24 Installing the rear cover with spacers



Step 6 Continue with the "NTP-12 Install Ferrites" procedure on page 1-59.

NTP-12 Install Ferrites

Purpose	This procedure describes how to attach ferrites.
Tools/Equipment	Oval and/or block ferrites
Prerequisite Procedures	NTP-6 Install the Power and Ground, page 1-23 NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-35
Required/As Needed	As needed
Onsite/Remote	Onsite

Step 1 To attach ferrites to power cabling, complete the "DLP-30 Install Ferrites to Power Cabling" task on page 1-59.

Step 2 To attach ferrites to wire-wrap pin fields, complete the "DLP-31 Attach Ferrites to Wire-Wrap Pin Fields" task on page 1-60.

Step 3 Continue with the "NTP-13 Perform the Shelf Installation Acceptance Test" procedure on page 1-61.

DLP-30 Install Ferrites to Power Cabling

Purpose	This task attaches ferrites to power cabling. Use a single oval ferrite TDK ZCAT2035-0930 and/or one block ferrite Fair Rite 0443164151 for each pair of cables, depending on the EIA.
Tools/Equipment	Oval and/or block ferrites
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite

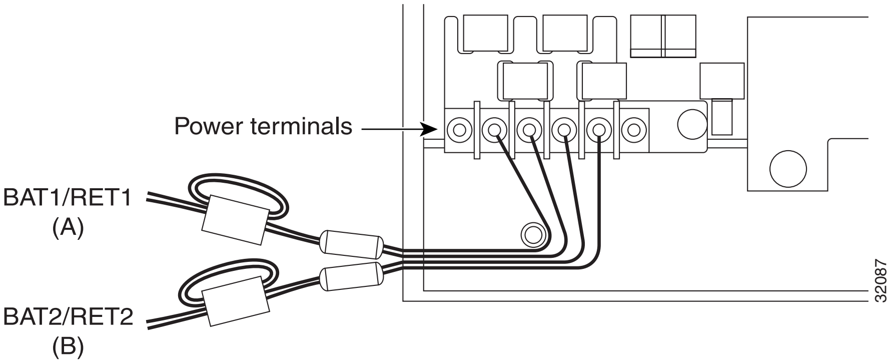
Step 1 If you are using block ferrites, wrap the cables once around and through the block ferrites.

Step 2 If you are using oval ferrites, pull the cable straight through the oval ferrites.

Note If you are using both block and oval ferrites, place the oval ferrite between the ONS 15454 and the block ferrite as shown in Figure 1-25 on page 1-60.

Note Place the oval ferrite as close to the power terminals as possible and place the block ferrite within 5 to 6 inches of the power terminals.

Figure 1-25 Attaching block and oval ferrites to power cabling



Step 3 Return to your originating procedure (NTP).

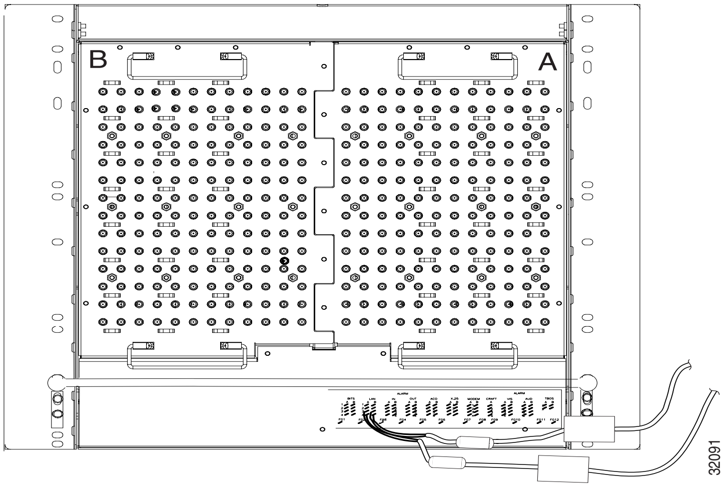
DLP-31 Attach Ferrites to Wire-Wrap Pin Fields

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 1-26 on page 1-61 shows the suggested method for attaching ferrites to wire-wrap pin fields.
Tools/Equipment	Oval and block ferrites
Prerequisite Procedures	NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-35
Required/As Needed	As needed
Onsite/Remote	Onsite

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. The block ferrite should be within 5 to 6 inches of the wire-wrap pin field.

Figure 1-26 Attaching ferrites to wire-wrap pin fields



Step 3 Return to your originating procedure (NTP).

NTP-13 Perform the Shelf Installation Acceptance Test

Purpose	Use this procedure to perform a shelf installation acceptance test.
Tools/Equipment	Voltmeter
Tools/Equipment	Oval and/or block ferrites
Prerequisite Procedures	Applicable procedures in Chapter 1
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Complete Table 1-9 on page 1-62 by verifying that each procedure was completed.

Table 1-9 ONS 15454 Shelf Installation Task Summary

Description	Completed
NTP-1 Unpack and Inspect the ONS 15454 Shelf Assembly, page 1-4	
NTP-2 Install the Shelf Assembly, page 1-5	
NTP-3 Open and Remove the Front Door, page 1-12	
NTP-4 Remove the Backplane Covers, page 1-15	
NTP-5 Install the Electrical Interface Assemblies, page 1-17	
NTP-6 Install the Power and Ground, page 1-23	
NTP-7 Install the Fan-Tray Assembly, page 1-29	
NTP-119 Install the Alarm Expansion Panel, page 1-31	
NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-35	
NTP-120 Install an External Wire-Wrap Panel to the AEP, page 1-42	
NTP-9 Install the Electrical Card Cables on the Backplane, page 1-47	
NTP-10 Route Electrical Cables, page 1-55	
NTP-11 Install the Rear Cover, page 1-57	
NTP-12 Install Ferrites, page 1-59	

Step 2 Complete the "DLP-32 Inspect the Shelf Installation and Connections" task on page 1-62.

Step 3 Complete the "DLP-33 Measure Voltage" task on page 1-63.

Step 4 Continue with the "NTP-15 Install the Common Control Cards" procedure on page 2-2.

DLP-32 Inspect the Shelf Installation and Connections

Purpose	This task inspects the shelf installation and connections to verify everything is installed and connected properly.
Tools/Equipment	None
Prerequisite Procedures	Complete Table 1-9 on page 1-62.
Required/As Needed	Required
Onsite/Remote	Onsite

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-33 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 1-62.
Required/As Needed	Required
Onsite/Remote	Onsite

Step 1 Using a voltmeter, verify the office ground and power (Figure 1-9 on page 1-27 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 -42 VDC and -57 VDC (power) and 0 (return ground).

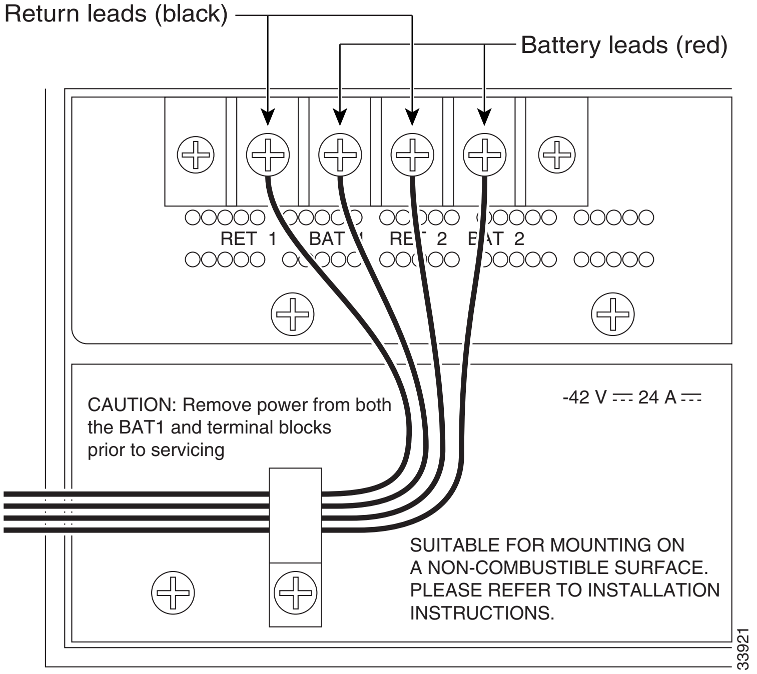
Step 2 Using a voltmeter, verify the shelf ground and power wiring:

a. Place the black lead (positive) on the RET1 and the red lead on the BAT1 point. Verify a reading between -42 VDC and -57 VDC. If there is no voltage, check the following:

- Battery and ground 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.

Figure 1-27 ONS 15454 power terminals


Return leads (black)
Battery leads (red)
RET 1
BAT 1
RET 2
BAT 2
CAUTION: Remove power from both the BAT1 and terminal blocks prior to servicing
-42 V ⎓ 24 A ⎓
SUITABLE FOR MOUNTING ON A NON-COMBUSTIBLE SURFACE. PLEASE REFER TO INSTALLATION INSTRUCTIONS.
33921

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. Before beginning any procedure in this chapter, make sure you have completed the "NTP-13 Perform the Shelf Installation Acceptance Test" procedure on page 1-61
2. NTP-15 Install the Common Control Cards, page 2-2—Complete this procedure before installing any other cards.
3. NTP-16 Install the Optical Cards, page 2-11—Complete this procedure as needed.
4. NTP-17 Install the Electrical Cards, page 2-13—Complete this procedure as needed.
5. NTP-18 Install the Ethernet Cards, page 2-14—Complete this procedure as needed.
6. NTP-116 Remove and Replace a Card, page 2-18—Complete this procedure as needed to remove and replace a card, including deleting the card from CTC and changing an optical card without losing the card's provisioning.
7. NTP-115 Pre-Provision a Slot, page 2-20—Complete this procedure as needed to provision an empty card slot with a card that will be installed later.
8. NTP-19 Install the Fiber-Optic Cables, page 2-20—Complete this procedure to install fiber on the optical cards or Ethernet GBICs and to route the fiber through the bottom of the shelf.
9. NTP-20 Replace the Front Door, page 2-30—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-15 Install the Common Control Cards

Purpose	This procedure describes how to install the common control cards.
Tools/Equipment	TCC+ cards XC/XCVT/XC10G (cross-connect) cards AIC/AIC-I card
Prerequisite Procedures	"NTP-13 Perform the Shelf Installation Acceptance Test" procedure on page 1-61
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 you install a card incorrectly, the FAIL LED will flash continuously.

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

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 to determine card/slot compatibility.

Step 2 Complete the "DLP-36 Install the TCC+ Cards" task on page 2-6.

Step 3 Complete the "DLP-37 Install the XC, XCVT, or XC10G Cards" task on page 2-8.

Step 4 Complete the "DLP-38 Install the Alarm Interface Controller or Alarm Interface Controller-International Card" task on page 2-10, if necessary.

Step 5 If you discover that you installed the wrong card in a slot, see the "NTP-116 Remove and Replace a Card" procedure on page 2-18.

Step 6 Proceed to the "NTP-16 Install the Optical Cards" procedure on page 2-11, the "NTP-17 Install the Electrical Cards" procedure on page 2-13, or the "NTP-18 Install the Ethernet Cards" procedure on page 2-14, as applicable for your site.

Table 2-1 ONS 15454 Card and Slot Compatibility

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**	**MS**	**MS**	**MS**	**HS**	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS**	**MS**	**MS**	**MS**
TCC+							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*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3-12	X	X	X	X	X	X						X	X	X	X	X	X
DS3-12E	X	X	X	X	X	X						X	X	X	X	X	X
DS3N-12	X*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3N-12E	X*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3XM-6	X	X	X	X	X	X						X	X	X	X	X	X
EC1-12	X	X	X	X	X	X						X	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-12-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.																
OC12 IR STM4 LH 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/4 STM4 SH 1310	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				
OC48 IR/STM16 SH AS 1310	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC48 LR/STM16 LH AS 1550	Not supported with XC/XCVT cards. Requires XC10G cards.																
OC48-ELR/STM 16 EH 100 GHz					X	X						X	X				

Table 2-1 ONS 15454 Card and Slot Compatibility (continued)

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Type	**MS**	**MS**	**MS**	**MS**	**HS**	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS**	**MS**	**MS**	**MS**
OC48 ELR 200 GHz					X	X						X	X				
OC192 LH/STM64 LH 1550	Not supported with XC/XCVT cards. Requires XC10G cards.																

MS identifies a multispeed slot.

HS identifies a high-speed slot.

X indicates that a card is supported in the slot.

X* identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.

Table 2-2 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**	**MS**	**MS**	**MS**	**HS**	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS**	**MS**	**MS**	**MS**
TCC+							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*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3-12	X	X	X	X	X	X						X	X	X	X	X	X
DS3-12E	X	X	X	X	X	X						X	X	X	X	X	X
DS3N-12	X*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3N-12E	X*	X*	X	X*	X*	X*						X*	X*	X*	X	X*	X*
DS3XM-6	X	X	X	X	X	X						X	X	X	X	X	X
EC1-12	X	X	X	X	X	X						X	X	X	X	X	X
E100T-12	Not supported with the XC10G card																
E1000-2	Not supported with the XC10G card																
E100T-12-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
OC12 IR STM4 LH 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/4 STM4 SH 1310	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				
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				

Table 2-2 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**	**MS**	**MS**	**MS**	**HS**	**HS**	**TCC**	**XC**	**AIC**	**XC**	**TCC**	**HS**	**HS**	**MS**	**MS**	**MS**	**MS**
OC48 ELR 200 GHz					X	X						X	X				
OC192 LH/STM64 LH 1550					X	X						X	X				

The XC10G card requires the ANSI shelf with high-speed fans.

MS identifies a multispeed slot.

HS identifies a high-speed slot.

X indicates that a card is supported in the slot.

X* identifies 1:N cards that operate as normal DS1 or DS3 cards when installed in certain slots.

DLP-36 Install the TCC+ Cards

Purpose	This task installs redundant TCC+ cards. The first card you install in the ONS 15454 must be a TCC+, and it must initialize before you install any cross-connect or traffic cards.
Tools/Equipment	Two TCC+ cards
Prerequisite Procedures	DLP-33 Measure Voltage, page 1-63
Required/As Needed	Redundant TCC+ cards are required.
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Open the latches/ejectors of the first TCC+ 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:

a. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.

b. The red FAIL LED blinks for 35 to 45 seconds.

c. The red FAIL LED remains illuminated for 5 to 10 seconds.

d. All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for 5 to 10 seconds.

e. The ACT/STBY LED turns on. (The ACT/STBY LED may take several minutes to illuminate while the DCC processor boots.)

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

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

Tip When a newly installed TCC+ card has a different version of the ONS 15454 software installed than the version running on the active TCC+, the newly-installed TCC+ card automatically copies the software version running on the active TCC+. You do not need to do anything in this situation. However, the loading TCC+ card will not boot up in the normal manner. When the card is first inserted, the red FAIL LED stays on for a short period. The FAIL LED then blinks normally and all LEDs go dark. The FAIL LED and the ACT/STBY LED flash alternately every 30 to 45 seconds as the new software loads onto the new TCC+ card. After loading the new software for approximately 30 minutes, the TCC+ card becomes the standby card and the amber LED is illuminated.

Step 5 Verify that the ACT/STBY LED is green for active. The IP address for the node, the temperature of the ONS 15454, and the time of day will be displayed 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 TCC+ card and install a replacement card.

Refer to the *Cisco ONS 15454 Software Upgrade Guide* or the "NTP-163 Restore the Node to Factory Configuration" procedure on page 15-11 to replace the software, or, to swap the TCC+, see the "NTP-116 Remove and Replace a Card" procedure on page 2-18.

Step 8 Open the latches/ejectors of the redundant TCC+ 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:

a. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds. If the red FAIL LED does not illuminate, check the power.

b. The red FAIL LED blinks for 35 to 45 seconds.

c. The red FAIL LED remains illuminated for 5 to 10 seconds.

d. All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for 5 to 10 seconds.

e. The ACT/STBY LED turns on. (The ACT/STBY LED may take several minutes to illuminate while the DCC processor boots.)

Note If the FAIL LED is illuminated continuously on the TCC+ card, see the tip in Step 4 about the TCC+ automatic upload.

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

Note Alarm LEDs may be illuminated; 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-37 Install the XC, XCVT, or XC10G Cards

Purpose	This task installs the XC/XCVT/XC10G cards.
Tools/Equipment	XC/XCVT/XC10G (cross-connect) cards
Prerequisite Procedures	DLP-36 Install the TCC+ Cards, page 2-6
Required/As Needed	Redundant cross-connect cards are required.
Onsite/Remote	Onsite

Note This is not the procedure to use when upgrading from XC to XCVT cards or from XCVT to XC10G cards. If you are performing an XC to XCVT upgrade or an XCVT to a XC10G upgrade, see Chapter 12, "Upgrade Cards and Spans."

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

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 (Slot 8 or 10).

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 as described below.

1. The red LED turns on and remains illuminated for 20 to 30 seconds.
2. The red LED blinks for 35 to 45 seconds.

3. The red LED remains illuminated for 5 to 10 seconds.
4. All LEDs blink once and turn on.
5. 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 illuminate, check the power.

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

Step 6 Verify that the ACT/STBY LED is green for active.

Step 7 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 8 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 9 Verify the LED activity as described below.

1. The red LED turns on and remains illuminated for 20 to 30 seconds.
2. The red LED blinks for 35 to 45 seconds.
3. The red LED remains illuminated for 5 to 10 seconds.
4. All LEDs blink once and turn on.
5. 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 illuminate, check the power.

Note If the red FAIL LED is illuminated continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 7 – 9.

Step 10 Verify that the ACT/STBY LED is amber for standby.

Step 11 Return to your originating procedure (NTP).

DLP-38 Install the Alarm Interface Controller or Alarm Interface Controller-International Card

Purpose	This task installs the AIC or AIC-I card.
Tools/Equipment	AIC or AIC-I card
Prerequisite Procedures	DLP-36 Install the TCC+ Cards, page 2-6 DLP-37 Install the XC, XCVT, or XC10G Cards, page 2-8
Required/As Needed	Required to use the ENVIR ALARMS (external alarms and controls) or orderwire functions. The AIC-I card can be used in both the ANSI and ETSI markets, while the AIC card is only used for ANSI.
Onsite/Remote	Onsite

Step 1 Open the latches/ejectors on the card.

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 (Slot 9).

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

- The red FAIL LED remains illuminated 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 6 If you have installed the AIC-I card, verify the following:

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

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

Note Before you insert a card into a slot provisioned for a different card, complete the "DLP-191 Delete a Card" task on page 2-18 for the previously provisioned card.

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

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

Step 7 Return to your originating procedure (NTP).

NTP-16 Install the Optical Cards

Purpose	This procedure describes how to install the optical 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-15 Install the Common Control Cards, page 2-2
Required/As Needed	Required if the node will carry optical traffic. Install according to site plan, if available.
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note To simplify UPSR to BLSR conversion and node addition, equip optical cards according to a high-speed east (Slots 12 and 13) and west (Slots 5 and 6) configuration. This configuration is not mandatory.

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.

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 optical cards except the OC192LR 1550 card, the laser is on even when the optical port is not in service. On the OC192LR 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).**

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

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 OC-192 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 optical card along the guide rails until the card plugs into the receptacle at the back of the slot.

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, as described below.

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/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 may not boot. If an optical card does not boot, open CTC and verify that the slot is not provisioned for a different card type before assuming the card is faulty.
- If the red FAIL LED does not illuminate, 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 illuminated continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 – 5.

Step 7 Complete the "NTP-19 Install the Fiber-Optic Cables" procedure on page 2-20.

Step 8 If you discover that you installed the wrong card in a slot, complete the "NTP-116 Remove and Replace a Card" procedure on page 2-18.

NTP-17 Install the Electrical Cards

Purpose	This procedure describes how to install the electrical cards (DS-1, DS-3, and EC1).
Tools/Equipment	Electrical cards
Prerequisite Procedures	NTP-15 Install the Common Control Cards, page 2-2 NTP-16 Install the Optical Cards, page 2-11 (if applicable)
Required/As Needed	Required if the node will carry any electrical traffic
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 Install higher-capacity cards first; for example, install a DS-3 card before installing a DS-1 card. Let each card completely boot before installing the next card.

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.

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:

1. The red FAIL LED turns on and remains illuminated for 10 to 15 seconds.

   If the red FAIL LED does not illuminate, check the power.

2. The red FAIL LED blinks for 30 to 40 seconds.
3. All LEDs blink once and turn off for 1 to 5 seconds.
4. 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.

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 illuminated continuously or the LEDs behave erratically, the card is not installed properly. Remove the card and repeat Steps 2 – 5.

Step 6 If you discover that you installed the wrong card in a slot, complete the "NTP-116 Remove and Replace a Card" procedure on page 2-18.

NTP-18 Install the Ethernet Cards

Purpose	This procedure describes how to install the Ethernet cards.
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-15 Install the Common Control Cards, page 2-2 NTP-16 Install the Optical Cards, page 2-11 (if applicable) NTP-17 Install the Electrical Cards, page 2-13 (if applicable)
Required/As Needed	Required if the node will carry Ethernet traffic
Onsite/Remote	Onsite

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.

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.**

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-39 Install Ethernet Cards" task on page 2-15. Allow each card to boot completely before installing the next card.

Note If you discover that you installed the wrong card in a slot, complete the "NTP-116 Remove and Replace a Card" procedure on page 2-18 and install the correct card.

Step 3 Complete the "DLP-40 Install Gigabit Interface Converters" task on page 2-16 if you are using E1000-2, E1000-2G, or G1000-4 cards.

DLP-39 Install Ethernet Cards

Purpose	This task installs the Ethernet cards.
Tools/Equipment	Ethernet cards
Prerequisite Procedures	DLP-36 Install the TCC+ Cards, page 2-6
Required/As Needed	Required
Onsite/Remote	Onsite

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, as described below.

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 1 to 5 seconds.
4. 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.

Note If the red FAIL LED does not illuminate, 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-40 Install Gigabit Interface Converters

Purpose	This task installs the gigabit interface converters (GBICs) and attaches fiber.
Tools/Equipment	GBICs
Prerequisite Procedures	DLP-39 Install Ethernet Cards, page 2-15
Required/As Needed	Required if you are using E1000-2, E1002-G, or G1000-4 cards.
Onsite/Remote	Onsite

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

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the part number (15454-GBIC-LX ,15454-GBIC-SX, or 15454-GBIC-2X) to verify that the GBIC is the correct type for your network.

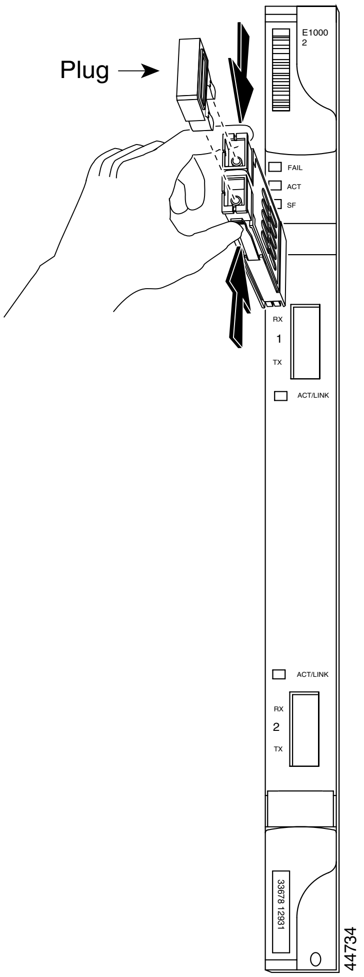
Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Grip the sides of the GBIC with your thumb and forefinger and insert it into the slot on the front panel of the Gigabit Ethernet card (shown in Figure 2-1 on page 2-17).

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

Note GBICs are keyed to prevent incorrect installation.

Figure 2-1 Installing a GBIC on an E1000-2 card



Step 5 Slide the GBIC through the cover flap until you hear a click.

The click indicates the GBIC is locked into the slot.

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

Step 7 Install and route the cable. See the "DLP-46 Route Fiber-Optic Cables" section on page 2-29 for routing instructions.

Step 8 Return to your originating procedure (NTP).

NTP-116 Remove and Replace a Card

Purpose	This procedure describes how to remove and replace cards in the ONS 15454 shelf.
Tools/Equipment	None
Prerequisite Procedures	None
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 (MEA) alarm with the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 If you are logged into CTC, either:

- Complete the "DLP-191 Delete a Card" task on page 2-18 and continue with Step 3 or
- Complete the "DLP-247 Change an Optical Card" task on page 2-19 to delete a card and replace it with a different optical 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-15 Install the Common Control Cards, page 2-2
- NTP-16 Install the Optical Cards, page 2-11
- NTP-17 Install the Electrical Cards, page 2-13
- NTP-18 Install the Ethernet Cards, page 2-14

DLP-191 Delete a Card

Purpose	This task deletes a card from CTC.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Both

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22. The node (default) view displays.

Step 2 On the shelf graphic, 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 TCC+ card
- The card is part of a protection group; see DLP-155 Delete a Protection Group, page 10-18
- The card has circuits; see NTP-152 Delete Circuits, page 9-11
- The card is part of a bidirectional line switched ring (BLSR); see NTP-161 Remove a BLSR Node, page 14-10
- The card is being used for timing; see DLP-157 Change the Node Timing Source, page 10-20
- The card has a SONET DCC termination; see DLP-156 Delete a SONET DCC Termination or Tunnel, page 10-19

Note If the card that was deleted is still installed in the shelf, it will reboot and re-appear in CTC.

Step 3 Return to your originating procedure (NTP).

DLP-247 Change an Optical Card

Purpose	This task describes how to change an optical card while maintaining existing provisioning, including DCCs, circuits, protection, timing, and rings. You cannot change a multiport card to a card with a smaller number of ports, and you cannot change a card to an identical card.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Physically removing an optical card can cause a loss of working traffic or a protection switch. See Chapter 12, "Upgrade Cards and Spans" for information on upgrading traffic to a higher speed.

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22. If you are already logged in, go to Step 2.

Step 2 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 3 In node view, right-click the card that you want to remove and choose **Change Card**.

Step 4 From the Change Card pull-down menu, choose the desired card type and click **OK**. A Mismatched Equipment Alarm (MEA) will appear until you replace the card.

Step 5 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 6 Complete the "NTP-16 Install the Optical Cards" procedure on page 2-11.

Step 7 Return to your originating procedure (NTP).

NTP-115 Pre-Provision a Slot

Purpose	This procedure describes how to pre-provision a slot in the software before physical card installation.
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 Log into the ONS 15454. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays. If you are already logged in, go to Step 2.

Step 2 Right-click the empty slot where you will later install a card.

Step 3 From the Add Card popup menu, choose the card type that will be installed.

Note When you pre-provision a slot, the card appears purple in the CTC shelf display, rather than white when a card is physically in the slot.

NTP-19 Install the Fiber-Optic Cables

Note You can install the fiber immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 5, "Turn Up Network."

Purpose	This procedure describes how to install fiber-optic cables on optical cards and Ethernet gigabit interface converters (GBIC).
Tools/Equipment	Fiber-optic cables Fiber boot
Prerequisite Procedures	NTP-16 Install the Optical Cards, page 2-11 NTP-18 Install the Ethernet Cards, page 2-14
Required/As Needed	Required
Onsite/Remote	Onsite

Note To install fiber-optic cables on an Ethernet card GBIC, see the "DLP-40 Install Gigabit Interface Converters" task on page 2-16.

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.

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 optical cards except the OC192LR 1550 card, the laser is on even when the optical port is not in service. On the OC192LR 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 1550 card unless you are using a 20 dB attentuator. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC-192 card.

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

Step 1 Test the optical receive levels for the cards installed and attenuate accordingly. See Table 2-3 for the minimum and maximum levels.

Table 2-3 Optical Transmit and Receive Levels

	Transmit		Receive	
Card	Minimum	Maximum	Minimum	Maximum
OC3 IR 4/STM1 SH 1310	–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/STM4-4	–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 LR/STM64 LH 1550	+7 dBm	+10 dBm	–19 dBm	–10 dBm

Step 2 As needed, complete the "DLP-207 Install Fiber-Optic Cables on the LGX Interface" task on page 2-23.

Step 3 Complete the "DLP-42 Install Fiber-Optic Cables on OC-N Cards" task on page 2-23.

Step 4 As needed, complete the "DLP-43 Install Fiber-Optic Cables for UPSR Configurations" task on page 2-24.

Step 5 As needed, complete the "DLP-44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-26.

Step 6 Complete the "DLP-45 Install the Fiber Boot" task on page 2-28.

Step 7 Complete the "DLP-46 Route Fiber-Optic Cables" task on page 2-29.

DLP-207 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-16 Install the Optical Cards, page 2-11 NTP-112 Clean Fiber Connectors, page 15-21
Required/As Needed	Required
Onsite/Remote	Onsite

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-112 Clean Fiber Connectors" procedure on page 15-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

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. See the "DLP-42 Install Fiber-Optic Cables on OC-N Cards" task on page 2-23.

Step 4 Return to your originating procedure (NTP).

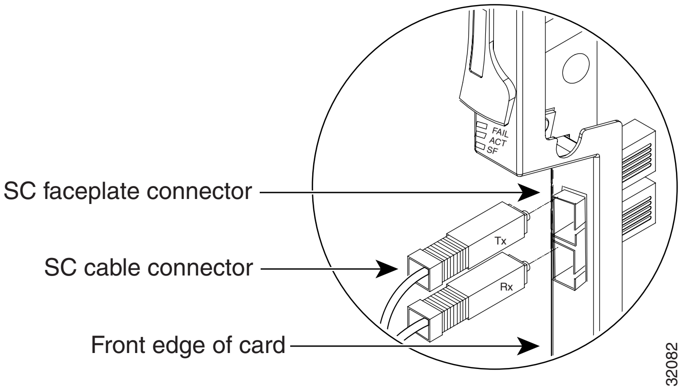
DLP-42 Install Fiber-Optic Cables on OC-N Cards

Purpose	This task installs fiber-optic cables on optical (OC-N) cards.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-16 Install the Optical Cards, page 2-11 NTP-112 Clean Fiber Connectors, page 15-21 DLP-207 Install Fiber-Optic Cables on the LGX Interface, page 2-23 (as applicable)
Required/As Needed	Required
Onsite/Remote	Onsite

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-112 Clean Fiber Connectors" procedure on page 15-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 1 Align the keyed ridge of the cable connector with the receiving SC connector on the faceplate connection point. Each card supports at least one transmit and one receive connector to create an optical carrier port. Figure 2-2 on page 2-24 shows the cable location.

Figure 2-2 Installing fiber-optic cables



Note The OC12/STM4-4 card faceplate has four ports.

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

Step 3 If you are installing fiber-optic cables on a OC12/STM4-4 card, repeat Steps 1 and 2 until all SC connectors are in place.

Step 4 Return to your originating procedure (NTP).

DLP-43 Install Fiber-Optic Cables for UPSR Configurations

Purpose	This task installs the fiber-optic cables to the east and west UPSR ports at each node. See Chapter 5, "Turn Up Network" to provision and test UPSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-16 Install the Optical Cards, page 2-11 NTP-112 Clean Fiber Connectors, page 15-21
Required/As Needed	Required
Onsite/Remote	Onsite

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.

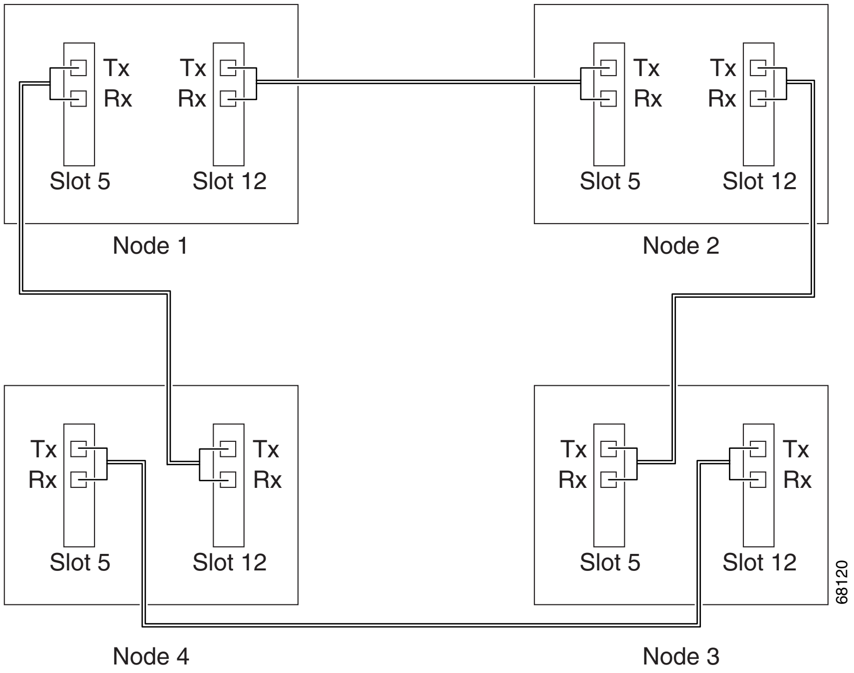
Note Inspect and clean all fiber connectors thoroughly. See the "NTP-112 Clean Fiber Connectors" procedure on page 15-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 1 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 will display a signal fail (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 2 Repeat Step 1 until you have configured the ring.

Figure 2-3 shows fiber connections for a four-node UPSR with trunk cards in Slot 5 (west) and Slot 12 (east).

Figure 2-3 Connecting fiber to a four-node UPSR



Step 3 Return to your originating procedure (NTP).

DLP-44 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 5, "Turn Up Network" to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-16 Install the Optical Cards, page 2-11 NTP-112 Clean Fiber Connectors, page 15-21
Required/As Needed	Required for a BLSR configuration
Onsite/Remote	Onsite

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.

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-112 Clean Fiber Connectors" procedure on page 15-21 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

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 will display a signal fail (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 will not function if working and protect cards are interconnected. See Figure 2-5 on page 2-28 for an example of correct four-fiber BLSR cabling.

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

Figure 2-4 shows fiber connections for a two-fiber BLSR with trunk cards in Slot 5 (west) and Slot 12 (east).

Figure 2-4 Connecting fiber to a four-node, two-fiber BLSR

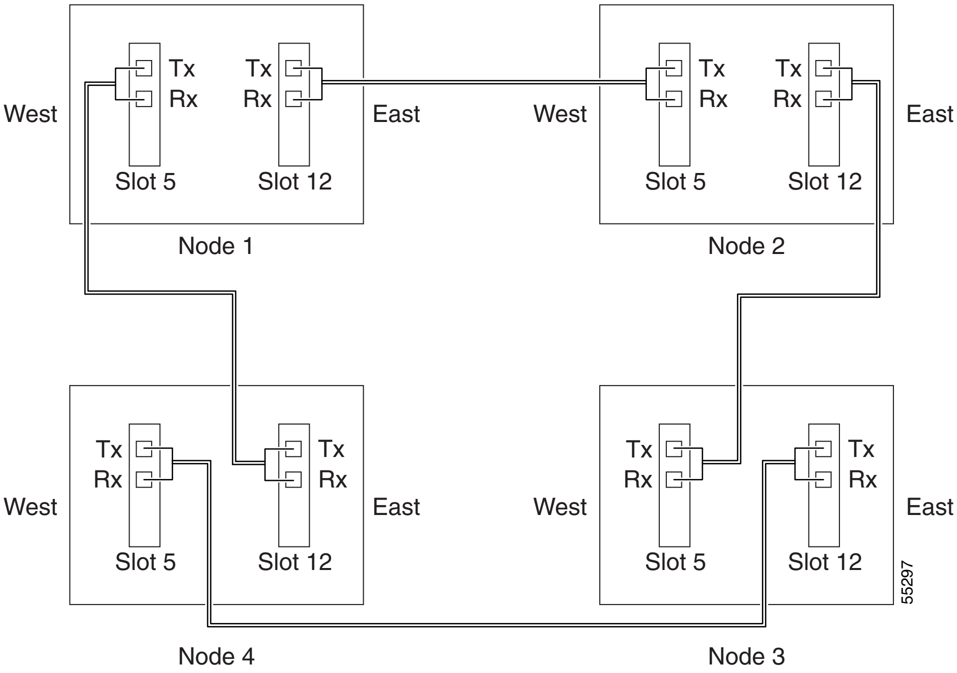
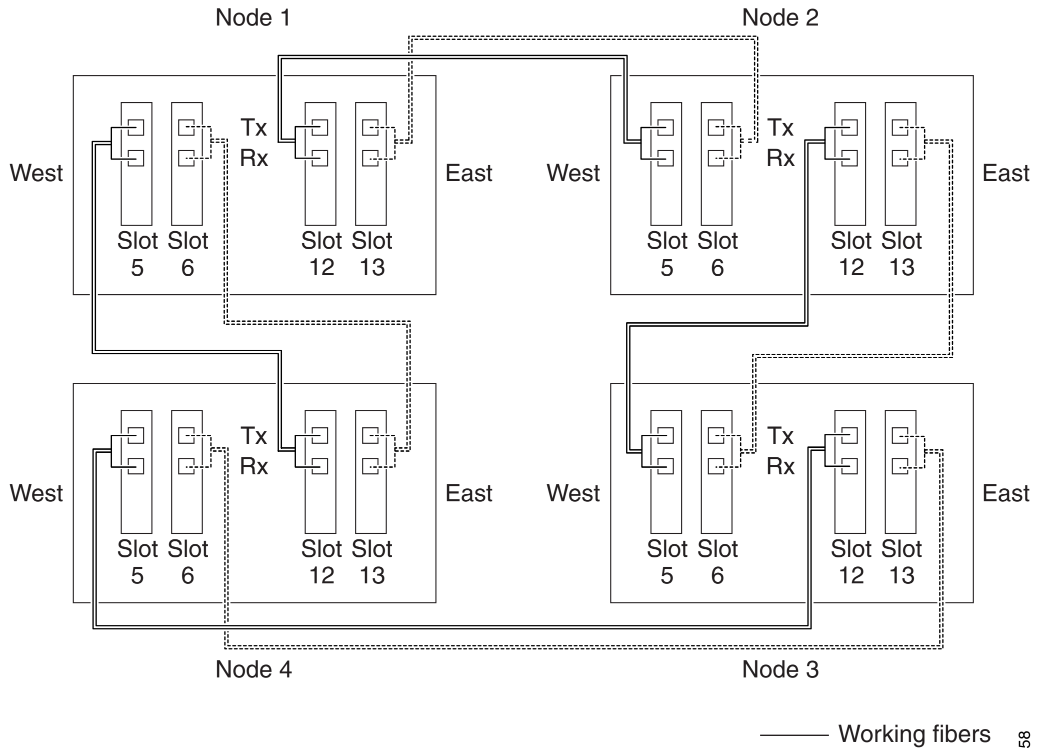


Figure 2-5 on page 2-28 shows fiber connections for a four-fiber BLSR. Slot 5 (west) and Slot 12 (east) carry the working traffic. Slot 6 (west) and Slot 13 (east) carry the protect traffic.

Figure 2-5 Connecting fiber to a four-node, four-fiber BLSR



Step 4 Return to your originating procedure (NTP).

DLP-45 Install the Fiber Boot

Purpose	This task installs the fiber boot.
Tools/Equipment	Fiber boot
Prerequisite Procedures	NTP-16 Install the Optical Cards, page 2-11 NTP-112 Clean Fiber Connectors, page 15-21
Required/As Needed	Required for all optical cards except the OC-192 and the OC-48 AS cards
Onsite/Remote	Onsite

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

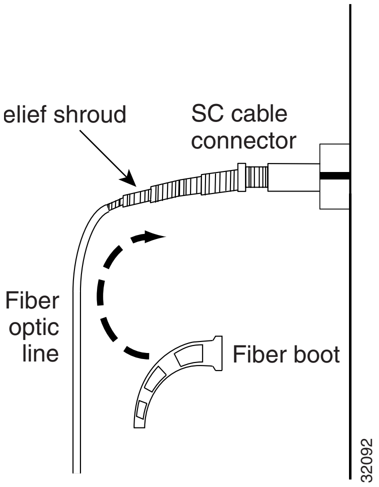
Step 1 Position the open slot of the fiber boot underneath the fiber cable.

Step 2 Push the fiber cable down into the fiber boot. Figure 2-6 on page 2-29 shows the fiber boot attachment.

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.

Figure 2-6 Attaching a fiber boot



Step 5 Return to your originating procedure (NTP).

DLP-46 Route Fiber-Optic Cables

Purpose	This task describes how to route fiber-optic cables.
Tools/Equipment	None
Prerequisite Procedures	Cables to be routed must be installed
Required/As Needed	Required
Onsite/Remote	Onsite

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. Fiber clips are factory-attached to the faceplate of the optical card.

GBICs do not have fiber clips; therefore, if you are routing optical cable from an E1000-2-G, E1000-2, or G1000-4 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.

Step 6 Return to your originating procedure (NTP).

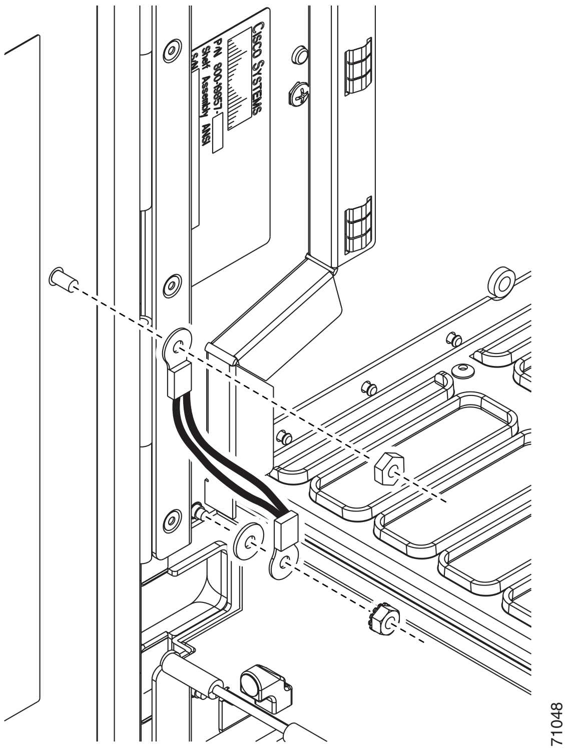
NTP-20 Replace the Front Door

Purpose	The following procedure explains how to replace the front door and door ground strap after installing cards and fiber-optic cables.
Tools/Equipment	#2 Phillips screw driver Medium slot head screw driver Small slot head screw driver
Prerequisite Procedures	Not applicable
Required/As Needed	As needed
Onsite/Remote	Onsite

Step 1 Insert the front door (removed in the "DLP-9 Remove the Front Door" task on page 1-13) 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. See Figure 2-7 on page 2-31.

Figure 2-7 Installing the Door Ground Strap Retrofit Kit

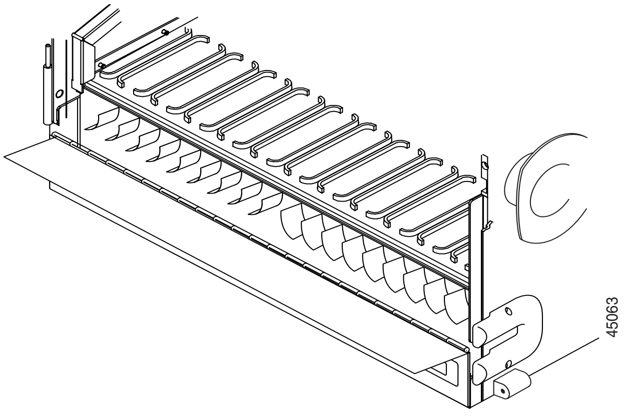


Step 3 Attach the other end of the ground strap to the longer screw on the fiber guide.

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.



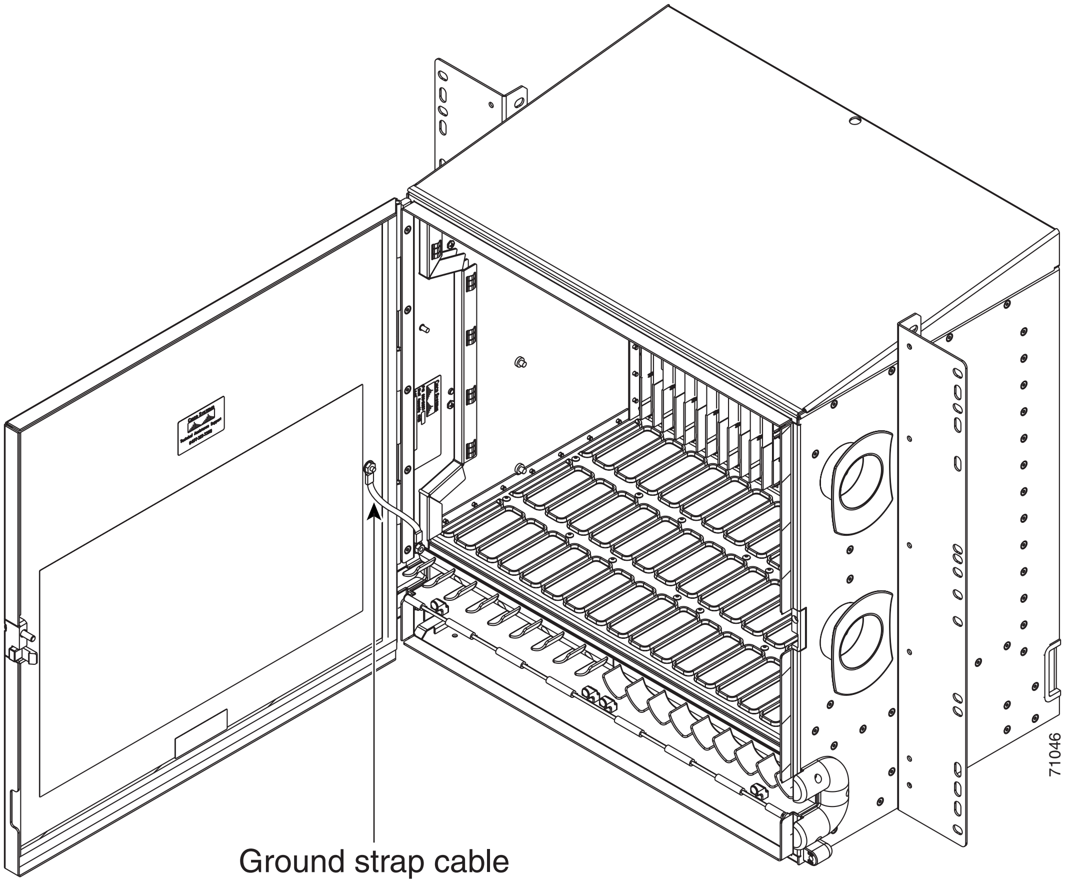
Note To avoid interference with the traffic (line) card, make sure the ground strap is in a flat position when the door is open. To move the ground strap into a flat position, rotate the terminal lug counterclockwise before tightening the Kepnut.

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 2-8 on page 2-32 shows the shelf assembly with the front door and ground strap installed.

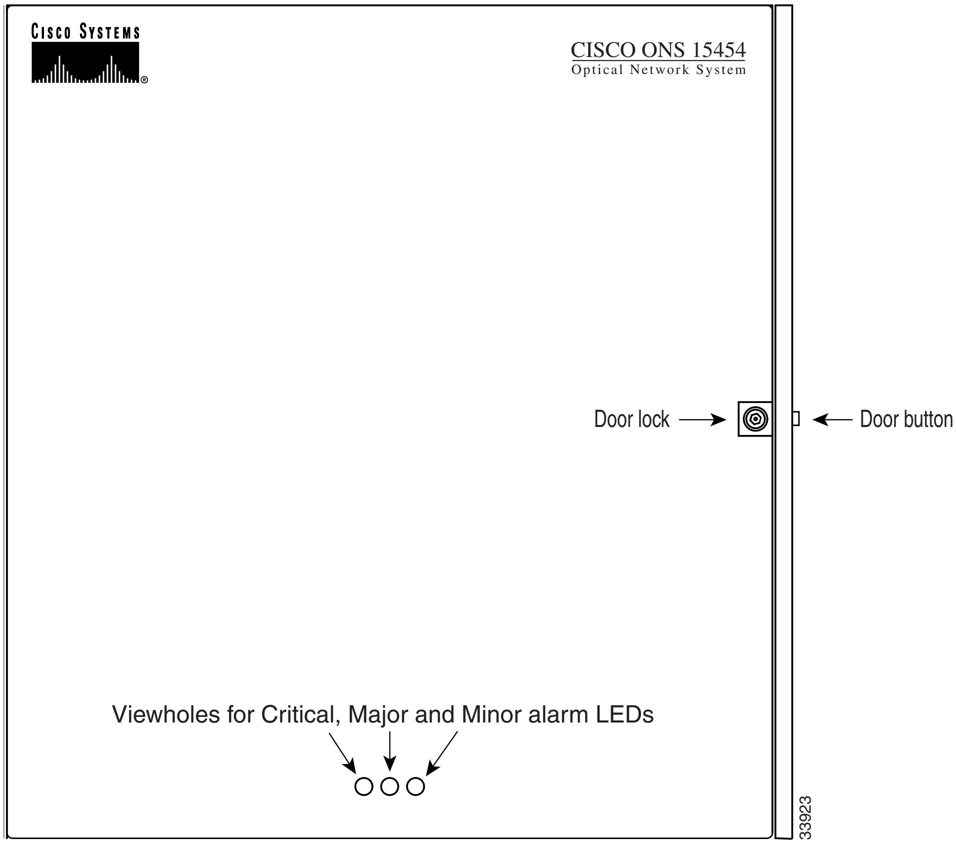
Figure 2-8 Shelf assembly with Door Ground Strap Retrofit Kit installed



Step 6 Swing the door closed. Figure 2-9 on page 2-33 shows the front door.

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.

Figure 2-9 The ONS 15454 front door



Step 7 Return to your originating procedure (NTP).

CHAPTER 3

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, the Cisco ONS 15454 OAM&P user interface.

Before You Begin

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

1. NTP-21 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-22 Set Up CTC Computer to Connect to the ONS 15454, page 3-8—After your PC or workstation is set up for CTC, complete this procedure to set up your computer to connect to the ONS 15454.
3. NTP-23 Log into the ONS 15454 GUI, page 3-21—Complete this procedure to log into CTC.

NTP-21 Set Up Computer for CTC

Purpose	This procedure explains how to configure your PC or UNIX workstation to run Cisco Transport Controller (CTC).
Tools/Equipment	Cisco ONS 15454 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote

Step 1 If your computer is a Windows PC, complete the "DLP-47 Run the CTC Installation Wizard for Windows" task on page 3-2, then go to Step 4.

Step 2 If your computer is a UNIX workstation, complete the "DLP-48 Run the CTC Installation Wizard for UNIX" task on page 3-5.

Step 3 If your computer is a UNIX workstation and you installed the JRE in Step 2, complete the "DLP-49 Set Up the Java Runtime Environment for UNIX" task on page 3-7.

Step 4 When your PC or workstation is set up, complete the "NTP-22 Set Up CTC Computer to Connect to the ONS 15454" procedure on page 3-8.

DLP-47 Run the CTC Installation Wizard for Windows

Purpose	This task installs CTC online help as well as programs required to run CTC on Windows PCs: Netscape 4.73 and JRE 1.3.1_02. It also modifies the Java Runtime Environment (JRE) policy file so CTC files can be downloaded to your computer when you connect to an ONS 15454.
Tools/Equipment	Cisco ONS 15454 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • Netscape Release 4.73 or later or Internet Explorer Release 4.0 (service pack 2) or later is not installed • JRE 1.3.1_02 is not installed • CTC online help is not installed and is needed • The JRE java.policy file has not been modified for CTC
Onsite/Remote	Onsite or remote

Step 1 Verify that your computer has the following:

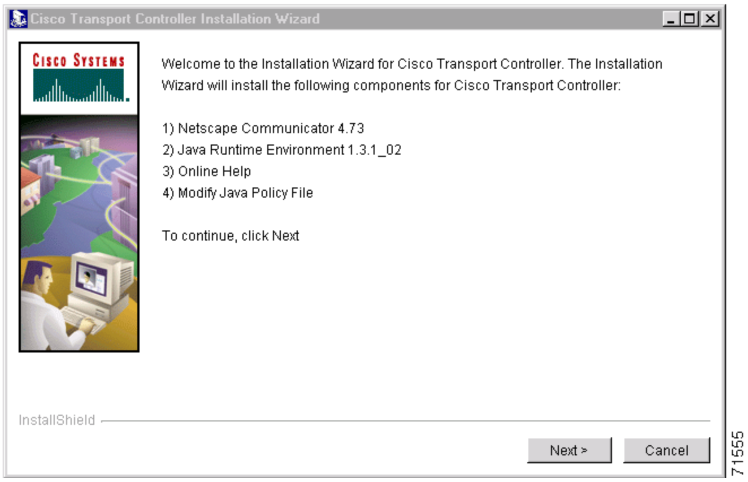
- Processor—Pentium II, 300 Mhz or faster
- RAM—128 MB
- Hard drive—2 GB is recommended. 50 MB of space must be available.
- Operating System—Windows 95, Windows 98, Windows NT 4.0, Windows 2000, or Windows XP. If your operating system is Windows NT, verify that Service Pack 5 or later is installed: 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 will be 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 3.4 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer (Figure 3-1).

Figure 3-1 Starting the Cisco Transport Controller Installation Wizard



Welcome to the Installation Wizard for Cisco Transport Controller. The Installation Wizard will install the following components for Cisco Transport Controller:

1) Netscape Communicator 4.73
2) Java Runtime Environment 1.3.1_02
3) Online Help
4) Modify Java Policy File

To continue, click Next

Step 3 Click **Next**.

Step 4 For installation type, choose **Typical** to install all the components shown in Figure 3-1, or choose **Custom** if you only want to install some of the components.

Step 5 Click **Next**.

Step 6 If you selected **Custom** in Step 4, select the CTC components you want to install and click **Next**. If you selected **Typical**, skip this step and proceed to Step 7.

Step 7 The directory where the installation wizard will install CTC online help is displayed. The default is C:\Program Files\Cisco\CTC\Documentation.

Step 8 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 and proceed to Step 9.

Step 9 Click **Next**.

Step 10 Review the components that will be installed. If you want to change them, click **Back**. If you have an active CTC session (for example, you are running the setup program to install additional components), close CTC before going to Step 11.

Step 11 Click **Next**.

An Installation Issues dialog box is displayed.

Step 12 Review the issues, then click **OK**. The InstallShield program begins the Netscape Communicator 4.73 Setup program.

Step 13 Complete the Netscape installation:

a. On the Netscape Communicator 4.73 Setup dialog box, click **Next**.

b. On the Software License Agreement dialog box, click **Yes**.

c. On the Setup Type dialog box, click **Typical**, then click **Next**.

Note If the Netscape installation hangs when installing RealPlayer G2, restart the CTC installation by pressing Ctrl+Alt+Del. On the Windows Security dialog box, click **Task Manager.** On the Windows Task Manager dialog box, click Cisco Transport Controller Installation Wizard, then click the **End Task** button. Click **Yes** on the confirmation. Navigate to the drive containing the CTC CD and double-click CTC.exe. Repeat Steps 1 – 12. At Step 13, substep c., click **Custom,** then click **Next.** At the next panel, deselect RealPlayer. Continue with substep d.

d. On the Netscape Desktop Preferences Options dialog box, check the boxes that apply according to your site requirements (these options will not affect CTC operation), then click **Next**.

e. On the Select Program Folder dialog box, click **Next**.

f. On the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.

g. On the Question dialog box, click **No**.

h. On the Information dialog box, click **OK**.

i. On the Restarting Windows dialog box, click **No, I will restart later**, then click **OK**.

Step 14 Close the Netscape Communicator directory window to display the Cisco Transport Controller Installation Wizard dialog box.

Step 15 On the CTC Installation Wizard dialog box, click **Next**. The Java 2 runtime environment installation begins.

Step 16 Complete the JRE installation:

a. On the Software License Agreement dialog box, click **Yes**.

b. On the Choose Destination Location dialog box, click **Next**.

c. On the Select Browser dialog box, click the Microsoft Internet Explorer and Netscape 6 checkboxes, then click **Next**.

When JRE installation is complete, the Cisco Transport Controller Installation Wizard dialog box is displayed.

Step 17 Click **Next**. The CTC online help is installed. When installed, the policy file selection is displayed.

Step 18 Choose the JRE policy file to modify:

- Choose **User Policy File** (default) to modify the policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only user who will access an ONS 15454 from the PC you are setting up, choose this option.
- Choose **System Policy File** to modify the system JRE policy file. This policy file applies to all computer users. If more than one individual will use this computer to access the ONS 15454, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

Step 19 Click **Next**.

Step 20 If you selected System Policy File in Step 18, complete the following steps. If you selected User Policy File, go to Step 21.

a. The System Policy File Update dialog box displays the default policy file location (C:\Program Files\JavaSoft\jre). If you installed the JRE in a different location, enter the new path in the Directory Name field. After entering the path, or if the default path is correct, click **OK**.

b. Click **OK** on the confirmation dialog box.

Step 21 Click **Finish**.

Step 22 To connect to the ONS 15454, restart your computer and complete the "NTP-22 Set Up CTC Computer to Connect to the ONS 15454" procedure on page 3-8.

DLP-48 Run the CTC Installation Wizard for UNIX

Purpose	This task installs CTC online help and programs required to run CTC on Solaris workstations: Netscape 4.76, JRE 1.3.1_02. It also modifies the Java Runtime Environment (JRE) policy file to allow CTC files to be downloaded to your computer after you connect to an ONS 15454.
Tools/Equipment	Cisco ONS 15454 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • Netscape Release 4.76 is not installed • JRE 1.3.1_02 is not installed • CTC online help is not installed and is needed • The JRE java.policy file has not been modified for CTC
Onsite/Remote	Onsite or remote

Step 1 Verify that your computer has the following:

- RAM—128 MB
- Hard drive—Verify that 50 MB of space is available.
- Operating System—Solaris 2.5.x or 2.6.x

Note These requirements are guidelines. CTC performance will be 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 (Figure 3-1 on page 3-3):

- Netscape Communicator 4.76
- Java Runtime Environment 1.3.1_02
- CTC Online Help
- Modify Policy File—The JRE java.policy file is modified to enable CTC to download files needed to run the Cisco Transport Controller when you connect to an ONS 15454.

Step 4 Click **Next**.

Step 5 For installation type, choose **Typical** to install all components, or choose **Custom** if you want to choose particular components to install.

Step 6 Click **Next**.

Step 7 If you selected the **Custom** in Step 5, choose the CTC components you want to install and click **Next**. If you selected **Typical**, proceed to Step 8.

Step 8 The directory where the installation wizard will install CTC online help is displayed. 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.

Step 9 Click **Next**.

Step 10 Review the components that will be installed. If you want to change them, click **Back**. If CTC is running (for example, you are reinstalling components) close CTC before going to the next step.

Step 11 Click **Next**. The InstallShield program begins the Netscape Communicator 4.76 Setup program.

Step 12 Complete the Netscape installation:

a. On the Netscape Communicator 4.76 Setup dialog box, click **Next**.

b. On the Software License Agreement dialog box, click **Yes**.

c. On the Setup Type dialog box, click **Typical**.

d. On the Netscape Desktop Preferences dialog box, check the boxes that apply, then click **Next**.

e. On the Program Folder, click **Next**.

f. On the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.

g. On the Question dialog box, click **No**.

Step 13 On the Cisco Transport Controller Installation Wizard dialog box, click **Next**. The Java 2 runtime environment installation begins.

Step 14 Complete the JRE installation:

a. On the Software License Agreement dialog box, click **Yes**.

b. On the Choose Destination Location dialog box, click **Next**.

c. On the Select Browser dialog box, click the Microsoft Internet Explorer and Netscape 6 checkboxes, then click **Next**.

When JRE installation is complete, the Cisco Transport Controller Installation Wizard dialog box is displayed.

Step 15 Click **Next**. The CTC online help is installed. When installed, the policy file selection is displayed.

Step 16 Choose the JRE policy file to modify:

- Choose **User Policy File** (default) to modify a policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only computer user who will access an ONS 15454, choose this option.
- Choose **System Policy File** to modify the system JRE policy file. This policy file applies to all computer users. If more than one individual will use this computer to access the ONS 15454, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

Step 17 Click **Next**, then click **Finish**.

Note Be sure to record the names of the directories you choose for Netscape, JRE, and the online documentation.

Step 18 If your installation included the JRE (that is, you chose the Typical installation or selected JRE from the custom installation), go to "DLP-49 Set Up the Java Runtime Environment for UNIX" task on page 3-7.

Note The Java Runtime Environment (JRE) may require certain patches to run properly. The patch tar file can be found in the JRE/Solaris directory on the CD. Please read the JRE/Solaris/Solaris.txt file for more information. In addition to installing any needed patches, follow the procedures below to set up JRE for use with Cisco Transport Controller on your UNIX system.

DLP-49 Set Up the Java Runtime Environment for UNIX

Purpose	Use this task to set up the Java Runtime Environment for UNIX workstations.
Tools/Equipment	None
Prerequisite Procedures	DLP-48 Run the CTC Installation Wizard for UNIX, page 3-5
Required/As Needed	Required if you installed the JRE during the CTC installation
Onsite/Remote	Onsite or remote

Note In this task, ***[your JRE path]*** represents the destination directory you chose for the Java Runtime Environment during JRE installation. For example, if your JRE destination directory is /usr/bin/jre, substitute /usr/bin/jre, wherever ***[your JRE path]*** occurs. Also, in the following procedures, ***[your Netscape path]*** refers to the destination directory you chose for Netscape, and must be substituted with your actual Netscape destination directory path.

Note CTC requires that the location of **xterm** is also in your path. If you have, for some reason, moved **xterm** from its default location, **/usr/openwin/bin**, you must change all occurrences of **/usr/openwin/bin** in the procedures below to reflect the actual path where **xterm** exists on your system.

Step 1 Set up the environment variable:

a. If you are using the csh shell, edit the .cshrc file in your home directory by appending the file with the lines:

setenv JRE [JRE path]

setenv NETSCAPE [Netscape path]

setenv NPX_PLUGIN_PATH $JRE/j2re1_3_1_02/plugin/sparc/ns4

set path = (/usr/openwin/bin $NETSCAPE $path)

b. If you are using the ksh or bash shell, edit the .profile file in your home directory by appending the file with the lines:

JRE=[your JRE path]

NETSCAPE=[your Netscape path]

NPX_PLUGIN_PATH=$JRE/j2re1_3_1_02/plugin/sparc/ns4

PATH=/usr/openwin/bin:$NETSCAPE:$PATH

export JRE NPX_PLUGIN_PATH PATH

Step 2 Set the JRE reference:

a. Run the Control Panel by typing:

[JRE path]/j2re1_3_0_02/bin/ControlPanel

b. Click the **Advanced** tab.

c. From the combo box, select **[JRE path]/j2re1_3_1_02**. If the JRE is not found, select **other** and enter **the following in the Path text box:**

[JRE path]/j2re1_3_1_02

d. Click **Apply**. Go to the "NTP-22 Set Up CTC Computer to Connect to the ONS 15454" procedure on page 3-8.

Note If you are running multiple shells, before your new environment variable will be set you may need to invoke the same shell for which you changed the initialization file (for example, if you added the environment variable to the .cshrc file, you must run your browser under the csh shell.

NTP-22 Set Up CTC Computer to Connect to the ONS 15454

Purpose	This procedure explains how to set up a PC running Windows or a Solaris workstation to connect to the ONS 15454.
Tools/Equipment	Depends on connection type
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 From Table 3-1, select the ONS 15454 connection type that you want to set up for your computer.

Note For initial shelf turn up, you should connect your PC directly to the LAN port on the TCC+ card of the ONS 15454.

Table 3-1 ONS 15454 Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15454 using: • The RJ-45 (LAN) port on the TCC+, or • The LAN pins on the ONS 15454 backplane, or • A hub or switch to which the ONS 15454 is connected.	• If you do not use DHCP, you will need to change the computer IP address, subnet mask, and default router.
Corporate LAN	Refers to a connection to the ONS 15454 through a corporate or NOC LAN.	• 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.
TL1	Refers to a connection to the ONS 15454 using TL1 rather than CTC. TL1 sessions can be started from CTC, or you can use a TL1 terminal. The physical connection can be a craft connection, corporate LAN, or a TL1 terminal. Refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.	
Remote	Refers to a connection made to the ONS 15454 using a modem.	• 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.

Step 2 If you need to set up your computer for corporate LAN access, complete the "DLP-55 Set Up a Computer for a Corporate LAN Connection" task on page 3-19. If not, proceed to the next step.

Step 3 If you need to set up the computer for remote access, complete the "DLP-58 Provision Remote Access to the ONS 15454" task on page 3-21. If not, proceed to the next step.

Step 4 If you need to set up your computer for TL1 access, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*. If not, proceed to the next step.

Step 5 If you need to set up your computer for local craft connections, choose a task from Table 3-2.

Table 3-2 ONS 15454 Craft Connection Options

Local Craft Connection Task	Description
• DLP-52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection, page 3-15	Complete this task if: • All nodes that you will access run software Release 3.3 or higher • 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 do not need to access or use non-ONS 15454 applications such as ping and trace route • You will connect to the ONS 15454's TCC+ ethernet port or backplane LAN pins either directly or through a hub
• DLP-50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses, page 3-11, or • DLP-53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454, page 3-17	Complete this task if: • You will access nodes running CTC software releases before Release 3.3 • You will connect to one ONS 15454; if you will connect to multiple ONS 15454s, you may need to configure your computer's IP settings each time you connect to an ONS 15454 • You need to access non-ONS 15454 applications such as ping and trace route
• DLP-51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using DHCP, page 3-13	Complete this task if: • The CTC computer is provisioned for DHCP • The ONS 15454 has DHCP forwarding enabled and is connected to a DHCP server

Step 6 After your computer is set up to connect to the ONS 15454, proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21.

DLP-50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses

Purpose	Use this task to set up your computer for a local craft connection to the ONS 15454 when: • You will access nodes running software releases before Release 3.3 • You will connect to one ONS 15454; if you will connect to multiple ONS 15454s, you may 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	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. On 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 95, Windows 98, Windows 2000, or Windows NT 4.0

Step 2 If you have Windows 95/98 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box select TCP/IP for your PC Ethernet card, then click **Properties**.

d. On 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 shown on the ONS 15454 LCD except for the last three digits. The last three digits must be between 1 and 254.

i. In the Subnet Mask field, type 255.255.255.0.

j. Click **OK**.

k. On 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 displays in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC displays, click **Yes**.

Step 3 If you have Windows NT installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On 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 three digits. The last three digits must be between 1 and 254.

g. In the Subnet Mask field, type 255.255.255.0.

h. Click the **Advanced** button.

i. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.

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 will prompt you to reboot your PC. If you receive this prompt, click **Yes**.

Step 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. On 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 three digits. The last three digits must be between 1 and 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. On the Local Area Connection Properties dialog box, click **OK**.

j. On the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

a. From the Windows Start Menu, choose **Control Panel > Network Connections**.

Note If the Network Connections icon 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 three digits. The last three digits must be between 1 and 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. On the Local Area Connection Properties dialog box, click **OK**.

i. On the Local Area Connection Status dialog box, click **Close**.

Step 6 After you set up your PC, proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using DHCP

Purpose	Use this task to set up your computer for craft connection to the ONS 15454 using DHCP (dynamic host configuration protocol).
Tools/Equipment	Straight-through (CAT-5) LAN cable
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1 NTP-26 Set Up CTC Network Access, page 4-5
Required/As Needed	As needed
Onsite/Remote	Onsite

Caution You will not be able to connect to the ONS 15454 if DHCP forwarding is not enabled on the ONS 15454 or the ONS 15454 is not connected to a DHCP server. By default, DHCP forwarding is not enabled. If you are connecting to an ONS 15454 to perform initial shelf turnup, complete the "DLP-50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses" task on page 3-11 or the "DLP-52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection" task on page 3-15.

Step 1 Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. On 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 95, Windows 98, Windows 2000, or Windows NT 4.0.

Step 2 If you have Windows 95/98 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box select TCP/IP for your PC Ethernet card, then click **Properties**.

d. On 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 from a DHCP Server**.

h. Click **OK**.

i. When the prompt to restart your PC displays, click **Yes**.

Step 3 If you have Windows NT installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On 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 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. On 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. On the Local Area Connection Properties dialog box, click **OK**.

g. On the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Control Panel> Network Connections**.

Note If the Network Connections icon is not available, click Switch to Classic View.

b. On the Network Connections dialog box, click **Local Area Connection**.

c. On 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 automatically**.

f. Click **OK**.

g. On the Local Area Connection Properties dialog box, click **OK**.

h. On the Local Area Connection Status dialog box, click **Close**.

Step 6 After you set up your PC, go to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection

Purpose	Use this task to set up your computer for local craft connection to the ONS 15454 when: • You will connect to the ONS 15454's 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 higher. • 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 trace route.
Tools/Equipment	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite

Note If you are using automatic host detection and you disconnect a straight-through (CAT-5) LAN cable from one node and connect it to another node, you must close CTC and relaunch it to reconnect to the proxy server and communicate with the new node.

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're in Classic View before continuing with this procedure.

b. On 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 95, Windows 98, Windows 2000, or Windows NT 4.0.

Step 2 If you have Windows 95/98installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box select TCP/IP for your PC Ethernet card, then click **Properties**.

d. On 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.

i. In the Subnet Mask field, type 255.255.255.0.

j. Click **OK**.

k. On the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the address entered in Step f. Click **Add**.

m. Verify that the IP address displays in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC displays, click **Yes**.

Step 3 If you have Windows NT installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Control Panel**.

b. On 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.

g. In the Subnet Mask field, type 255.255.255.0.

h. Click the **Advanced** button.

i. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.

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 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. On 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.

f. In the Subnet Mask field, type 255.255.255.0.

g. Type the IP address entered in Step e in the Gateway Address field.

h. Click **OK**.

i. On the Local Area Connection Properties dialog box, click **OK**.

j. On the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

a. From the Windows Start Menu, choose **Control Panel > Network Connections**.

Note If the Network Connections icon 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.

e. In the Subnet Mask field, type 255.255.255.0.

f. Type the IP address entered in Step d in the Gateway Address field.

g. Click **OK**.

h. On the Local Area Connection Properties dialog box, click **OK**.

i. On the Local Area Connection Status dialog box, click **Close**.

Step 6 After you set up your PC, you can go to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454

Purpose	Use this task to set up a Solaris workstation for a craft connection to the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite

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

a. 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. Go to Step 4.

b. If the interface is not plumbed, a message similar to the following appears: ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface. Plumb the interface by typing:

```
# if config <device> plumb
```

For example: ifconfig hme1 plumb

Step 3 Configure the IP address on the interface by typing:

```
#ifconfig <interface> <ip address> netmask <netmask> up
```

For example: #ifconfig hme0 10.20.30.40 netmask 255.255.255.0 up

Note Enter an IP address that is identical to the ONS 15454 IP address except for the last three digits. The last three digits must be between 1 and 254. In the Subnet Mask field, type 255.255.255.0. Skip this step if "Craft Access Only" from **Provisioning** > **Network** > **General** > **Gateway Settings** is checked.

Step 4 Test the connection:

a. Start Netscape Navigator.

b. Enter the Cisco 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 display. If this occurs, go to Step 2 of the "DLP-60 Log into CTC" task on page 3-22 to complete the login. If the Login dialog box does not appear, complete Steps c–d.

c. At the prompt, type:

ping [ONS 15454 IP address]

For example, you would type "ping 192.168.1.1" to connect to an ONS 15454 with default IP address 192.168.1.1. If your workstation is connected to the ONS 15454, an "[IP address] is alive" message displays.

Note Skip this step if "Craft Access Only" from **Provisioning** > **Network** > **General** > **Gateway Settings** is checked.

d. If CTC is not responding, a "Request timed out" message displays. Verify IP and submask 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

The result of 1 means the link is up. The result of 0 means the link is down.

Note Check the man page for ndd. For example: **#man ndd**

Step 5 After you set up your workstation, proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-55 Set Up a Computer for a Corporate LAN Connection

Purpose	Use this task to set up your computer to access the ONS 15454 through a corporate LAN.
Tools/Equipment	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 If your computer is 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 95/98) or "Obtain an IP address from a DHCP server" (Windows NT/2000/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 the task for the web browser you use:

- DLP-56 Disable Proxy Service Using Internet Explorer (Windows), page 3-19, or
- DLP-57 Disable Proxy Service Using Netscape (Windows and UNIX), page 3-20

DLP-56 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote

Step 1 From the Start menu, select **Settings > Control Panel**.

Note If you computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure you're in Classic View before continuing with this procedure.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 From the Internet Properties dialog box, click **Connections** > **LAN Settings**.

Step 4 On the LAN Settings dialog box, either:

- Deselect **Use a proxy server** to disable the service, or

- Leave **Use a proxy server** selected and click **Advanced**. On 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 Proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-57 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a proxy server and your browser is Netscape.
Onsite/Remote	Onsite or remote

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, either:

- Choose **Direct connection to the Internet** to bypass the proxy server

or

- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. On 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 Proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

DLP-58 Provision Remote Access to the ONS 15454

Purpose	Use this task to connect an ONS 15454 using a LAN modem.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote

Step 1 Connect the modem to the RJ-45 (LAN) port on the TCC+ or to the LAN pins on the ONS 15454 backplane.

Step 2 Refer to the modem documentation 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 at 1-877-323-7368.

Step 3 Proceed to the "NTP-23 Log into the ONS 15454 GUI" procedure on page 3-21 to log into the ONS 15454.

NTP-23 Log into the ONS 15454 GUI

Purpose	Use this procedure to log into the Cisco Transport Controller, the graphical user interface software used to manage the ONS 15454. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1 NTP-22 Set Up CTC Computer to Connect to the ONS 15454, page 3-8
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 If the computer is not connected to the ONS 15454, complete the"DLP-59 Connect Computer to the ONS 15454" task on page 3-22.

Step 2 Complete the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Note For information about navigating in CTC, see Appendix A.

Step 3 As needed, complete the "DLP-61 Create Login Node Groups" task on page 3-24. Login node groups display nodes that are not connected to the log-in node via DCC.

Step 4 As needed, complete the "DLP-62 Add a Node to the Current Session or Login Group" task on page 3-25.

DLP-59 Connect Computer to the ONS 15454

Purpose	Use this task to connect a CTC computer to the ONS 15454.
Tools/Equipment	Straight-through (CAT-5) LAN cable
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
	NTP-22 Set Up CTC Computer to Connect to the ONS 15454, page 3-8
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote

Step 1 If your computer is set up for a local craft connection, connect a straight-through (CAT-5) LAN cable from the PC or Solaris workstation NIC card to one of the following:

- The RJ-45 (LAN) port on the TCC+
- The 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 (CAT-5) LAN cables, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 If your computer is set up for a corporate LAN connection, connect a straight-through (CAT-5) LAN from the PC or Solaris workstation NIC card to a LAN port.

Step 3 Continue to the "DLP-60 Log into CTC" task on page 3-22.

DLP-60 Log into CTC

Purpose	Use this task to log into the Cisco Transport Controller, the graphical user interface software used to manage the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-21 Set Up Computer for CTC, page 3-1
	NTP-22 Set Up CTC Computer to Connect to the ONS 15454, page 3-8
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.

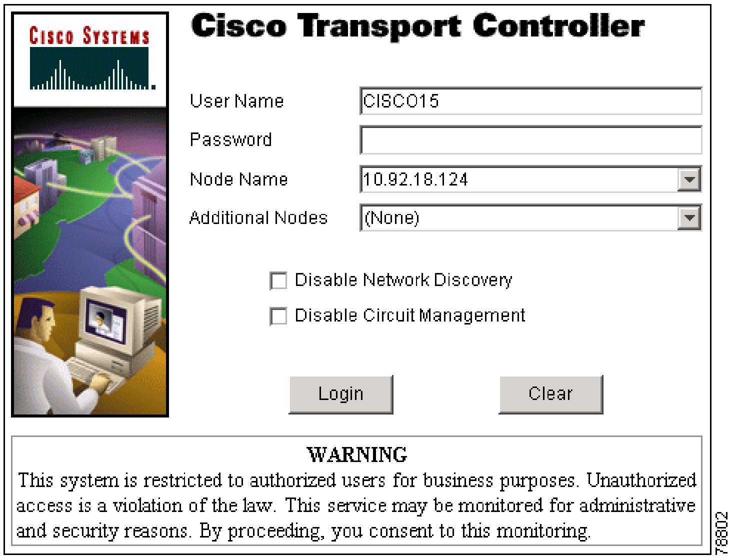
Step 1 From the PC connected to the ONS 15454, start Netscape or Internet Explorer.

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 address, 192.1.0.2. (This IP address should be displayed on the LCD.) Press **Enter**.

Note If you are logging into ONS 15454 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node with an older release, you receive an INCOMPATIBLE-SW alarm and the IP address of the login node will display instead of the node name. To check the software version of a node, select **About CTC** from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages display while CTC files are downloaded to your computer. The first time you connect to an ONS 15454, this process can take several minutes. After the download, the CTC Login dialog box displays (Figure 3-2).

Figure 3-2 Logging into CTC



Cisco Transport Controller

User Name: CISCO15

Password:

Node Name: 10.92.18.124

Additional Nodes: (None)

□ Disable Network Discovery

□ Disable Circuit Management

WARNING
This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

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" if it is not already displayed.

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 without a password. To create a password for CISCO 15, 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-30 Create Users and Assign Security" procedure on page 4-28. Additional information is provided in the *Cisco ONS 15454 Reference Guide*.

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 pull-down menu of previously-entered ONS 15454 IP addresses. You can select any ONS 15454 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- *Additional Nodes*—Displays a list of login node groups that were created. To create a login node group or add additional groups, see the "DLP-61 Create Login Node Groups" task on page 3-24.)

Note Topology hosts that were created in previous ONS 15454 releases by modifying the ctc.ini (Windows) or .ctcrc (UNIX) files are displayed as a "Topology Host" group under Additional Nodes.

- *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 the *Node Name* ONS 15454 through the DCC are not displayed. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.
- *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 login is successful, the CTC window displays. From here, you can navigate to other CTC views to provision and manage the ONS 15454. If you need to perform the initial shelf turn up, see Chapter 4, "Turn Up Node." If login problems occur, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

DLP-61 Create Login Node Groups

Purpose	Create 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	NTP-21 Set Up Computer for CTC, page 3-1
	NTP-22 Set Up CTC Computer to Connect to the ONS 15454, page 3-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the network. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 From the Edit menu, choose **Preferences**.

Step 3 Click **Login Node Group** and **Create Group**.

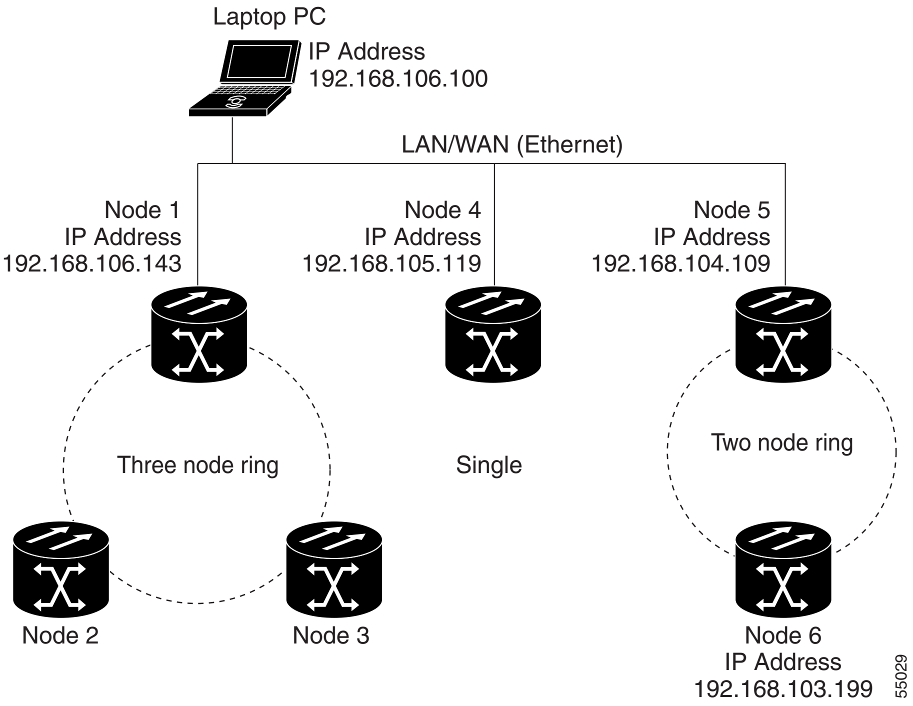
Step 4 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

Step 5 Under Members, 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 you want to add to the group.

Step 6 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 3-3, a login node group, "Test Group," is created and the IP addresses for Nodes 1, 4, and 5. During login, if you select Test Group under *Additional Nodes* and Disable Network Discovery is not selected, all nodes in the figure are displayed. If Test Group and Disable Network Discovery are both selected, Nodes 1, 4, and 5 will be displayed. 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 3-3 A login node group



DLP-62 Add a Node to the Current Session or Login Group

Purpose	Use this task to add a node to the current CTC session or login node group.
Tools	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the network. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 From the CTC File menu, click **Add Node** (or click the Add Node button on the toolbar).

Step 3 On the Add Node dialog box, enter the node name (or IP address).

Step 4 If you want to add the node to the current login group, click **Add Node to Current Login Group**. Otherwise, leave it unchecked.

Note The Add Node to Current Login Group checkbox is active only if you selected a login group when you logged into CTC.

Step 5 Click **OK**.

After a few seconds, the new node will be displayed on the network view map.

CHAPTER 4

Turn Up Node

This chapter explains how to provision a single Cisco ONS 15454 node and turn it up for service.

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-24 Verify Card Installation, page 4-2—Complete this procedure first.
2. NTP-25 Set Up Name, Date, Time, and Contact Information, page 4-3—Continue with this procedure to set the node name, date, time, location, and contact information.
3. NTP-26 Set Up CTC Network Access, page 4-5—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
4. NTP-27 Set Up the ONS 15454 for Firewall Access, page 4-15—Continue with this procedure if the ONS 15454 will be accessed behind firewalls.
5. NTP-28 Set Up Timing, page 4-18—Continue with this procedure to set up the node’s SONET timing references.
6. NTP-30 Create Users and Assign Security, page 4-28—Complete this procedure to create CTC users and assign their security levels.
7. NTP-121 Set the Port Name for a Card, page 4-31—Complete this procedure, as needed, to assign names to the ports on the cards.
8. NTP-29 Create Protection Groups, page 4-23—Complete this procedure, as needed, to set up 1:1, 1:N, and 1+1 protection groups for ONS 15454 electrical and optical cards.
9. NTP-32 Provision the Alarm Interface Controller, page 4-31—Complete this procedure if an AIC card is installed in Slot 9 and you want to set up external (environmental) alarms, controls, or orderwire.
10. NTP-123 Provision the Alarm Interface Controller-International, page 4-35Complete this procedure if an AIC-I card is installed in Slot 9 and you want to set up external (environmental) alarms, controls, or orderwire.

11. NTP-33 Set Up SNMP, page 4-38—Complete this procedure if SNMP will be used for system monitoring.

NTP-24 Verify Card Installation

Purpose	This procedure verifies that the ONS 15454 node 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 TCC+ cards are installed in Slots 7 and 11.

Step 2 Verify that the green ACT (active) LED is illuminated on one TCC+ and the amber STBY (standby) LED is illuminated on the second TCC+.

Note If the TCC+s are not installed, or their LEDs are not illuminated as described, do not proceed. Repeat the "DLP-36 Install the TCC+ Cards" task on page 2-6, or refer to the *Cisco ONS 15454 Troubleshooting Manual* to resolve installation problems before proceeding to Step 3.

Step 3 Verify that cross-connect cards (XC, XCVT, or XC10G) are installed in Slots 8 and 10.

Note The OC-192, OC48 any-slot (AS), four-port OC-12, and G1000-4 cards require an XC10G. If the OC48 AS cards are not installed in high-speed slots, they can operate with an XC or XCVT card.

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 their LEDs are not illuminated as described, do not proceed. Repeat the "DLP-36 Install the TCC+ Cards" task on page 2-6, or refer to the *Cisco ONS 15454 Troubleshooting Manual* to resolve installation problems before proceeding to Step 5.

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 the ONS 15454 multispeed or high-speed slots as designated by your installation plan.

Note Multispeed slots are Slots 1–4 and 14–17; high-speed slots are Slots 5, 6, 12, and 13.

Step 7 If your site plan requires an Ethernet card, verify that the Ethernet card is installed in the specified multispeed or high-speed slot and its ACT (active) LED displays a solid green light.

Step 8 If a E1000-2, E1000-2-G, or G1000-4 Ethernet card is installed, verify that it has a gigabit interface converter (GBIC) installed. If not, see the "DLP-40 Install Gigabit Interface Converters" task on page 2-16.

Step 9 Verify that OC-N cards (OC-3, OC-12, OC-12-4, OC-48, OC-48AS, and OC-192) are installed in the slots designated by your site plan. OC-3, OC-12, and OC-48AS cards can be installed in multispeed or high-speed slots. The OC-12-4 can only be installed in a multispeed slot, and the OC-48 and OC-192 can only be installed in high-speed slots.

Note Multispeed slots are Slots 1–4 and 14–17; high-speed slots are Slots 5, 6, 12, and 13.

Step 10 Verify that all installed OC-N cards display a solid amber STBY LED.

Step 11 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan.

Step 12 Verify that fiber is routed correctly in the shelf assembly and fiber boots are installed properly.

Step 13 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 procedure using a Cisco ONS 15445 software CD. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for instructions.
- Replace the TCC+ cards with cards containing the correct release (see the " NTP-116 Remove and Replace a Card" procedure on page 2-18).
- Use the " NTP-163 Restore the Node to Factory Configuration" procedure on page 15-11.

Step 14 Continue with the " NTP-25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-3.

NTP-25 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-24 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-60 Log into CTC" task on page 3-22 for the node you will turn up.

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 characters.

- *Contact*—Type the name of the node contact person and the phone number (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 by pressing **Ctrl**, then clicking and dragging the node icon to the desired location with your mouse.

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 (.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 *Use NTP/SNTP Server*, type the IP address of either a) an NTP/SNTP server, or b) the IP address of an ONS 15454 with NTP/SNTP Server enabled. If you enable *Enable Firewall* for the ONS 15454 proxy server, external ONS 15454 NEs must reference the gateway ONS 15454 NE for NTP/SNTP timing. For more information about the proxy server feature, 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 selected, 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 selected, 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 popup 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 (Mountain), and GMT-08 (Pacific).

Step 4 Click **Apply**.

Step 5 On the confirmation dialog box, click **Yes**.

Step 6 Review the node information. If you need to make corrections, repeat Steps 3–5 to enter the corrections. If the information is correct, continue with the " NTP-26 Set Up CTC Network Access" procedure on page 4-5.

NTP-26 Set Up CTC Network Access

Purpose	Use this procedure to provision network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP listener port, proxy server settings, static routes, open shorted path first (OSPF) protocol, and routing information protocol (RIP).
Tools/Equipment	None
Prerequisite Procedures	NTP-24 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-60 Log into CTC" task on page 3-22. If you are already logged in, from the View menu in node (default) view select **Go to Network View**.

Step 2 Complete the "DLP-63 Provision IP Settings" task on page 4-6 to provision the ONS 15454 IP address, subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP listener port, and proxy server settings.

Tip If you cannot log into the node, you can still change its IP address, default router and network mask by using the LCD on the ONS 15454 front panel. See the "DLP-64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-9 for instructions. However, you cannot use the LCD to provision any other network settings.

Step 3 If static routes are needed, complete the "DLP-65 Create a Static Route" task on page 4-11. 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-66 Set Up or Change Open Shortest Path First Protocol" task on page 4-12.

Step 5 If the ONS 15454 is connected to a LAN or WAN that uses RIP, complete the "DLP-248 Set Up or Change Routing Information Protocol" task on page 4-14.

DLP-63 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	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution All network changes should be approved by your network (or LAN) administrator.

Step 1 If you are in network view, switch to node view by double-clicking the node you want to turn up on the network map.

Step 2 Click the **Provisioning** > **Network** tabs.

Step 3 Complete the following information in the fields listed:

- *IP Address*—Type the IP address assigned to the ONS 15454 node.
- *Prevent LCD IP Config*—Check this box if you want to disable IP configuration using the ONS 15454 LCD, that is, disable the "DLP-64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-9. This box is unchecked by default.
- *Default Router*—If the ONS 15454 must communicate with a device on a network that the ONS 15454 is not connected to, the ONS 15454 may forward the packets to the default router. Type the IP address of the router in this field. If the ONS 15454 is not connected to a LAN, or if you will enable any of the *Gateway Settings* to implement the ONS 15454 proxy server features, leave this field blank.
- *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.
- *MAC Address*—(read only) Displays the ONS 15454 IEEE 802 Media Access Control (MAC) address.
- *Forward DHCP Request To*—Check this box to enable Dynamic Host Configuration Protocol (DHCP). Also, enter the DHCP server IP address in the *Request To* field. The box is unchecked by 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.

- *TCC CORBA (IIOP) Listener Port*—Check this box to set the ONS 15454 IIOP listener port. This listener port is used to allow communication with the ONS 15454 through firewalls. See the " NTP-27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-15 to provision firewall access.
- *Gateway Settings*—Provides three checkboxes that enable the ONS 15454 proxy server features. Do not enable any of the checkboxes until you review the proxy server scenario in the *Cisco ONS 15454 Reference Manual*. In proxy server networks, the ONS 15454 will be either a gateway network element (GNE) or external network element (ENE). Provisioning must be consistent for each NE type.
  - Craft Access Only— If checked, the login ONS 15454 is only visible to the CTC workstation that it is directly connected to; other non-DCC connected nodes will not be aware of the node provisioned for craft access only. This box is normally checked for external NEs; not checked for gateway NEs. If Craft Access Only is checked, Enable Proxy must be selected in order for the directly connected PC to have visibility to DCC-connected nodes.
  - Enable Proxy—If checked, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes for which it serves as a proxy. Both gateway and external NEs within a proxy server network should have this box checked.
  - Enable Firewall—If checked, the node restricts IP traffic from being routed between the DCC and the LAN port. Both gateway and external NEs within a proxy server network should have this box checked. If Enable Firewall is checked, Enable Proxy must be selected in order for the directly connected PC to have visibility to DCC-connected nodes.

Step 4 Click **Apply**.

Step 5 Click **Yes** on the confirmation dialog box.

Both ONS 15454 TCC+ cards will reboot, one at a time. During this time (approximately 10–15 minutes), the active and standby TCC+ LEDs will go through the cycle shown in Table 4-1 on page 4-8. Eventually, a "Lost node connection, switching to network view" message is displayed.

Table 4-1 LED Behavior During TCC+ Reboot

Active TCC+ LEDs	Standby TCC+ LEDs	Reboot Activity
ACT/STBY: flashing green	1. ACT/STBY: flashing yellow 2. FAIL LED: solid red 3. FAIL LED: flashing red 4. Alarm LEDs: flash once 5. ACT/STBY: flashing yellow 6. All LEDs: turn off (1-2 minutes) 7. ACT/STBY: solid yellow 8. ACT/STBY: Solid green	Standby TCC+ updated with new network information
1. FAIL LED: solid red 2. FAIL LED: flashing red 3. Alarm LEDs: flash once 4. ACT/STBY: flashing yellow 5. All LEDs: turn off (1-2 minutes) CTC displays “Lost node connection, switching to network view” message 6. ACT/STBY: solid yellow	ACT/STBY: solid green	Active TCC+ updated with new network information If an AIC card is installed, AIC FAIL and alarm LEDS light up briefly when the AIC is updated
ACT/STBY: solid yellow	ACT/STBY: solid green	The backup TCC+ becomes the active TCC+

Step 6 Click **OK**. CTC displays the network view. The node icon is displayed in grey, during which time you cannot access the node.

Step 7 Double-click the node icon when it changes to green. As necessary, complete the “DLP-65 Create a Static Route” task on page 4-11 or the “DLP-66 Set Up or Change Open Shortest Path First Protocol” task on page 4-12. If you do not need to create a static route or set up OSPF, go to the “ NTP-28 Set Up Timing” procedure on page 4-18.

DLP-64 Set the IP Address, Default Router, and Network Mask Using the LCD

Purpose	Use this task to change the ONS 15454 IP address, default router, and network mask using the front panel LCD. Use this task if you cannot log into CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-36 Install the TCC+ Cards, page 2-6
Required/As Needed	Optional
Onsite/Remote	Onsite
Security Level	N/A

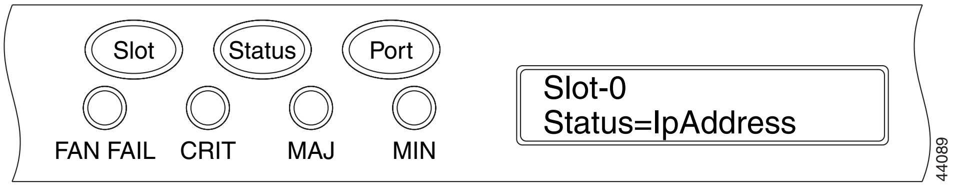
Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

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

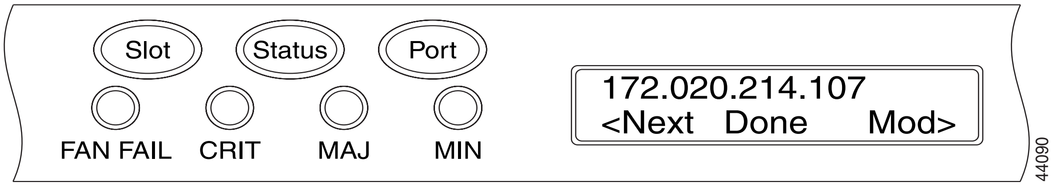
Figure 4-1 Selecting the IP address option



```
Slot-0
Status=IpAddress
```

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



```
172.020.214.107
<Next   Done      Mod>
```

Step 4 Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

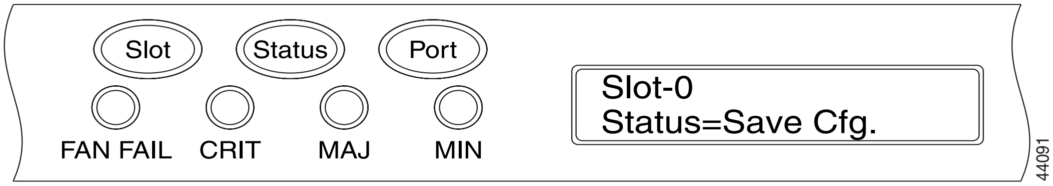
Tip The Slot, Status, and Port button positions correspond to the command position on the LCD. For example, in Figure 4-2, you press the Slot button to invoke the Next command and the Port button to invoke the Done command.

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

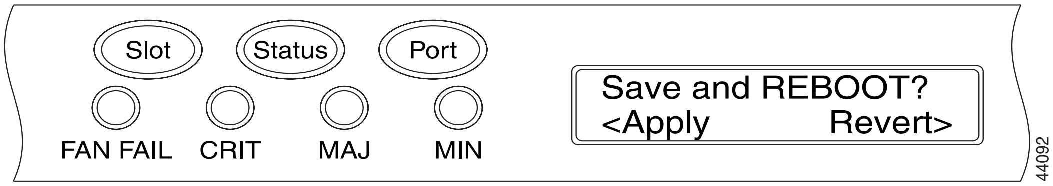


```
Slot-0
Status=Save Cfg.
```

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 TCC+



```
Save and REBOOT?
<Apply          Revert>
```

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 TCC+ 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 TCC+ reboot is complete (see Table 4-1 on page 4-8 for reboot behavior).

Note The IP address and default router must be configured to be on the same subnet. If not, you cannot apply the configuration.

Step 10 Return to your originating procedure (NTP).

DLP-65 Create a Static Route

Purpose	Use this task to create a static route on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required if either of the following is true: • You need to connect ONS 15454s to CTC sessions on one subnet connected by a router to ONS 15454s residing on another subnet when OSPF is not enabled, and the Enable Proxy box are not checked. • You need to enable multiple CTC sessions among ONS 15454s residing on the same subnet, when the Craft Access Only feature is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the network view (from the View menu in node view click **Go to Network View**).

Step 2 Click the **Provisioning** > **Network** tabs.

Step 3 Click the **Static Routing** tab. Click **Create**.

Step 4 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 *Destination* is a host route (i.e., one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If *Destination* is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If *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 5 Click **OK**. Verify that the static route displays 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 6 Return to your originating procedure (NTP).

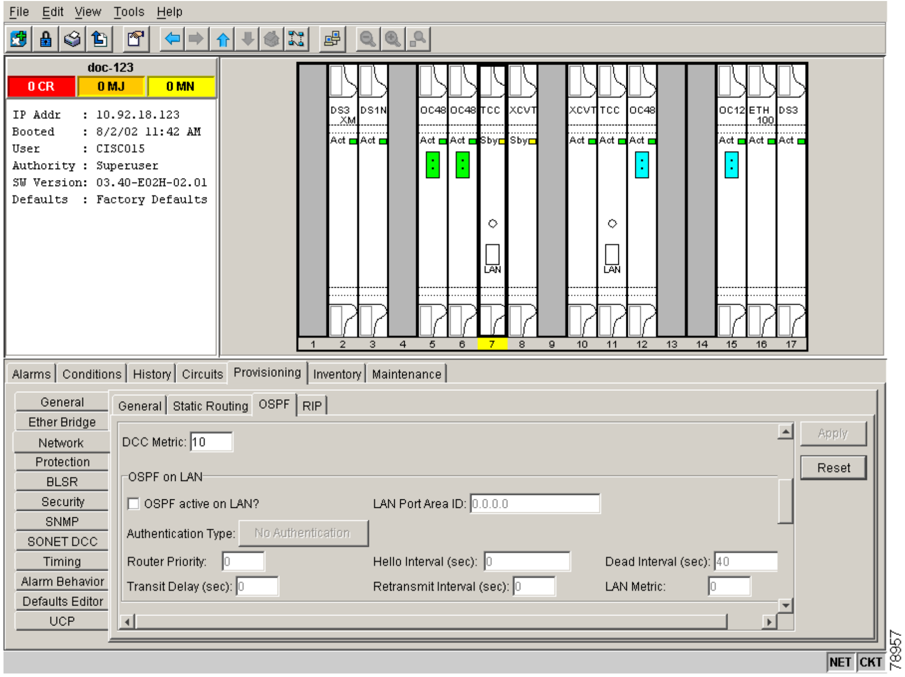
DLP-66 Set Up or Change Open Shortest Path First Protocol

Purpose	Use this task to enable 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	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router that the ONS 15454 is connected to.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node view.

Step 2 Click the **Provisioning** > **Network** > **OSPF** tabs (Figure 4-5).

Figure 4-5 Enabling OSPF on the ONS 15454



doc-123

0 CR 0 MJ 0 MN

```
IP Addr   : 10.92.18.123
Booted    : 8/2/02 11:42 AM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

DCC Metric: 10

OSPF on LAN

□ OSPF active on LAN? LAN Port Area ID: 0.0.0.0

Authentication Type: No Authentication

Router Priority: 0 Hello Interval (sec): 0 Dead Interval (sec): 40

Transit Delay (sec): 0 Retransmit Interval (sec): 0 LAN Metric: 0

Step 3 On the top left side of the OSPF pane, complete the following:

- *DCC OSPF Area ID Table*—Enter the number that identifies the ONS 15454s as a unique OSPF area ID entered in dotted decimal format. It can be any number between 000.000.000.000 and 255.255.255.255. The number must be unique to the LAN OSPF area.

- *DCC Metric*—This value is normally unchanged. It sets a “cost” for sending packets across the DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default DCC metric is 10. The metric changes to 100 if you check the *OSPF Active on LAN* checkbox in Step 4.

Step 4 Under OSPF on LAN, 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 OSPF Area ID.)

Step 5 Under **Authentication**, complete the following:

- *Type*—If the router where the ONS 15454 is connected requires authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- *Key*—If Simple Password is selected as the Authentication type, enter the password (OSPF key).

Step 6 Under **Priority and Intervals**, complete the following:

The OSPF priority and intervals default to values most commonly used by OSPF routers. In the Priority and Intervals area, verify that these values match those used by the OSPF router where the ONS 15454 is connected.

- *Router Priority*—Used to select 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 7 Under **OSPF Area Range Table**, create an area range table if one is needed:

Note Area range tables consolidate the information that is propagated 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 8 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 9 After entering ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the TCC+ cards will reset, one at a time. The reset will take approximately 10-15 minutes. Table 4-1 on page 4-8 shows the LED behavior during the TCC+ reset.

Step 10 Return to your originating procedure (NTP).

DLP-248 Set Up or Change Routing Information Protocol

Purpose	Use this task to enable 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	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22 You need to create a static route to the router adjacent to the ONS 15454 in order 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 Display the node view.

Step 2 Click the **Provisioning** > **Network** > **RIP** tabs.

Step 3 Check the RIP Active? checkbox if you are activating RIP.

Step 4 Choose either RIP Version 1 or RIP Version 2 from the drop down menu, depending on which version is supported in your network.

Step 5 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 6 Under **Authentication**, select the authentication type; If the router where the ONS 15454 is connected requires authentication, choose **Simple Password**. Otherwise, choose **No Authentication**. (default). You must click the No Authentication button to choose the Simple Password option.

Step 7 Return to your originating procedure (NTP).

NTP-27 Set Up the ONS 15454 for Firewall Access

If an ONS 15454 or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15454 and/or CTC computer, depending on whether one or both devices reside behind a firewall.

Figure 4-6 shows ONS 15454s in a protected network and the CTC computer in an external network. In order for the computer to access the ONS 15454s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15454. The ONS 15454 sends the port number to the CTC computer during the initial contact between the devices using Hyper-Text Transfer Protocol (HTTP). After the CTC computer obtains the ONS 15454 IIOP port, the computer opens a direct session with the node using the specified IIOP port.

Figure 4-6 ONS 15454s residing behind a firewall

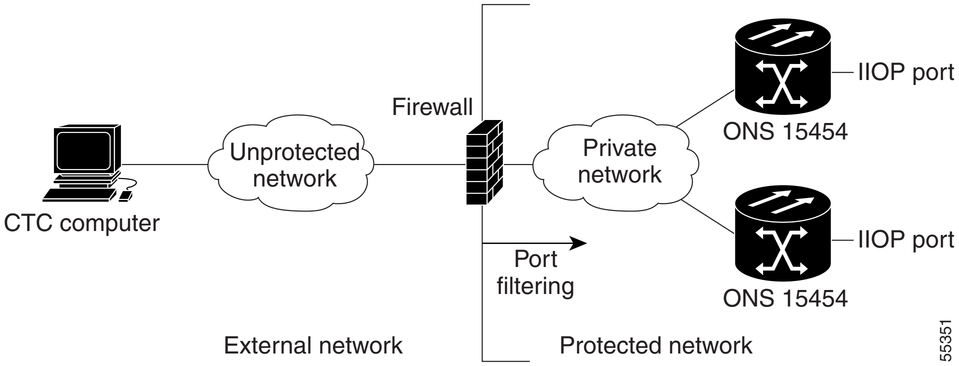
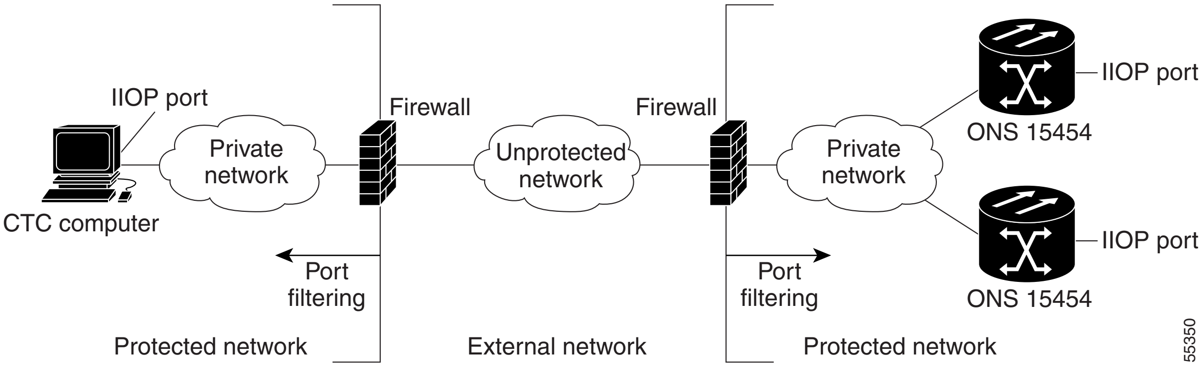


Figure 4-7 shows a CTC computer and ONS 15454 behind firewalls. In order for the computer to access the ONS 15454, you provision the IIOP port on the CTC computer and on the ONS 15454. Each firewall can use a different IIOP port. For example, if the CTC computer firewall uses IIOP port 4000, and the ONS 15454 firewall uses IIOP port 5000, 4000 is the IIOP port set on the CTC computer and 5000 is the IIOP port set on the ONS 15454.

Figure 4-7 A CTC computer and ONS 15454s residing behind firewalls



Purpose	This procedure provisions ONS 15454s and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator
Prerequisite Procedures	NTP-24 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-60 Log into CTC" task on page 3-22 for instructions.

Step 2 If the ONS 15454 resides behind a firewall, complete the "DLP-67 Provision the IIOP Listener Port on the ONS 15454" task on page 4-16.

Step 3 If the CTC computer resides behind a firewall, complete the "DLP-68 Provision the IIOP Listener Port on the CTC Computer" task on page 4-18.

DLP-67 Provision the IIOP Listener Port on the ONS 15454

Purpose	Use this task to 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 from LAN or firewall administrator
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Provisioning** > **Network** tabs.

Step 2 On the **General** subtab under TCC+ CORBA (IIOP) Listener Port, choose a listener port option:

- *Default - TCC Fixed*—Uses Port 57790. Used to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This 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 TCC+

Port	Function
0	Never used
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 TCC+
2361	TL1
3082	TL1
3083	TL1
5001	BLSR server port
5002	BLSR client port
7200	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC boot port
9999	Flash manager
10240-12288	Proxy client
57790	Default TCC listener port

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration? message displays, click **Yes**.

Both ONS 15454 TCC+s will reboot, one at a time. The reboot will take approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-68 Provision the IIOP Listener Port on the CTC Computer

Purpose	Use this task to select the IIOP listener port on CTC.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
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 On the Preferences dialog box, click the **Firewall** tab.

Step 3 Under CTC CORBA (IIOP) Listener Port, choose a listener port option:

- *Default - Variable*—Used to connect to ONS 15454s from within a firewall or if no firewall is used (default)
- *Standard Constant*—Uses 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 is displayed telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 On the Preferences dialog box, click **OK**. A warning is displayed telling you that the port change will apply on the next CTC login.

Step 7 Click **OK**.

Step 8 To access the ONS 15454 using the IIOP port, log out of CTC (from the File menu, select **Exit**), then log into the ONS 15454.

Step 9 Return to your originating procedure (NTP).

NTP-28 Set Up Timing

Purpose	Use this procedure to provision the ONS 15454 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 node where you want to set up timing. The node (default) view displays. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Complete the"DLP-69 Set Up External or Line Timing" task on page 4-19 if an external BITS source is available. This is the common SONET timing setup procedure.

Step 3 Complete the"DLP-70 Set Up Internal Timing" task on page 4-22 if you cannot complete Step 2 (an external BITS source is not available). This task can only provide Stratum 3 timing.

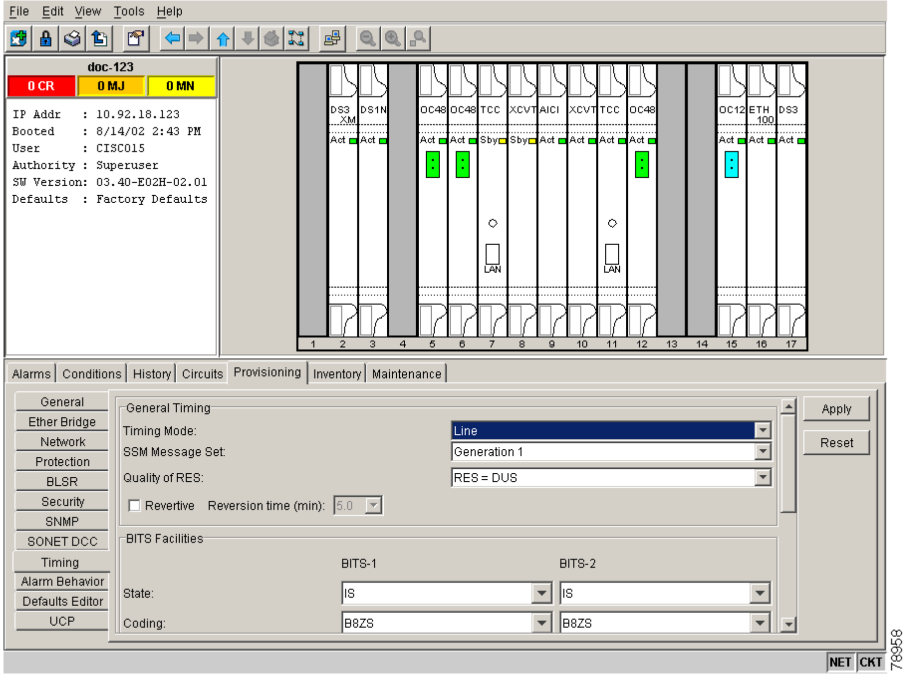
Note For information about SONET timing, refer to the *Cisco ONS 15454 Reference Guide* or to Telcordia GR-253-CORE.

DLP-69 Set Up External or Line Timing

Purpose	Use this task to define the SONET timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the node view, click the **Provisioning > Timing** tabs (Figure 4-8).

Figure 4-8 Setting Up ONS 15454 timing



```
IP Addr   : 10.92.18.123
Booted    : 8/14/02 2:43 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

General Timing

Timing Mode: Line

SSM Message Set: Generation 1

Quality of RES: RES = DUS

□ Revertive Reversion time (min): 5.0

BITS Facilities

	BITS-1	BITS-2
State:	IS	IS
Coding:	B8ZS	B8ZS

Step 2 Under General Timing, 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 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 may cause timing loops, Cisco does not recommend its use. Use this mode with care.

- *SSM Message Set*—Choose the message set level supported by your network. If a Generation 1 node receives a Generation 2 message, the message will be mapped down to the next available Generation 1. For example, an ST3E message becomes an ST3.
- *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 Guide* for more information about SSM, including definitions of the SONET timing levels.
- *Revertive*—Check this 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 back to its primary timing source. Five minutes is the default.

Step 3 Under BITS Facilities, complete 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.

- *State*—For nodes set to Line timing with no equipment timed through BITS Out, set *State* to OOS (Out of Service). For nodes using External timing or Line timing with equipment timed through BITS Out, set *State* to IS (In Service).

Step 4 If State is set to OOS, go to Step 5. If *State* is set to IS, complete the following information:

- *Coding*—Set to the coding used by your BITS reference, either B8ZS or AMI.
- *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 Super Frame.
- *AIS Threshold*—If SSM is disabled or Super Frame 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 sent 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 it and the ONS 15454. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft.

Note LBO does not appear in releases before Release 3.3.

Step 5 Under Reference Lists, 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.

- *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 that fails, the node uses Reference 3, which is typically set to Internal Clock. This is the Stratum 3 clock provided on the TCC+. The options displayed depend on the *Timing Mode* setting.
  - If the *Timing Mode* is set to External, your options are BITS1, BITS2, and Internal Clock.
  - If the *Timing Mode* is set to Line, your options are the node's working OC-N cards 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 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*—Define the timing references for equipment wired to the BITS Out backplane pins. Normally, BITS Out is used with Line nodes, so the options displayed are the working OC-N cards. BITS 1 and BITS 2 Out are enabled when BITS-1 and BITS-2 facilities are placed in service.

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-70 Set Up Internal Timing

Purpose	Use this task to set up internal timing (Stratum 3) for an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
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 Click the **Provisioning > Timing** tabs.

Step 2 Under General Timing, enter the following:

- *Timing Mode*—Set to External
- *SSM Message Set*—Set to Generation 1
- *Quality of RES*—Not applicable to internal timing
- *Revertive*—Not relevant for internal timing; the default setting (checked) is sufficient
- *Revertive Time*—The default setting (5 minutes) is sufficient

Step 3 Under BITS Facilities, change State to OOS (Out of Service)

- *Coding*—Not relevant for internal timing; the default (B8ZS) is sufficient
- *Framing*—Not relevant for internal timing; the default (ESF) is sufficient
- *Sync Messaging*—Not relevant for internal timing
- *AIS Threshold*—Not relevant for internal timing
- *LBO*—Not relevant for internal timing.

Step 4 Under Reference Lists, 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 Log into a node that will be timed from the node set up in Steps 1–5.

Step 7 Click the **Provisioning > Timing** tabs.

Step 8 In the General Timing section, enter the same information as entered in Step 3 with the following exceptions:

- *Timing Mode*—Set to Line

Reference Lists

- *NE Reference*
  - Ref1—Set to the OC-N trunk card with the closest connection to the node in Step 3
  - Ref 2—Set to the OC-N trunk card with the next closest connection to the node in Step 3
  - Ref 3—Set to Internal Clock

Step 9 Click **Apply**.

Step 10 Repeat Steps 6–9 at each node that will be timed by the node in Step 3.

Step 11 Return to your originating procedure (NTP).

NTP-29 Create Protection Groups

Purpose	Use this procedure to create ONS 15454 card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2
Required/As Needed	Required; some network information is optional, depending on your site plan
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 node where you want to create the protection group. The node (default) view displays. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Complete one or more of the following tasks depending on the protection group(s) you want to create:

- DLP-71 Create a 1:1 Protection Group, page 4-24
- DLP-72 Create a 1:N Protection Group, page 4-26
- DLP-73 Create a 1+1 Protection Group, page 4-27

Note Table 4-3 describes the protection types available on the ONS 15454.

Table 4-3 Card 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 TCC+, 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: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.
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.
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.

DLP-71 Create a 1:1 Protection Group

Purpose	Use this task to create 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	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
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 Click the **Provisioning** > **Protection** tabs.

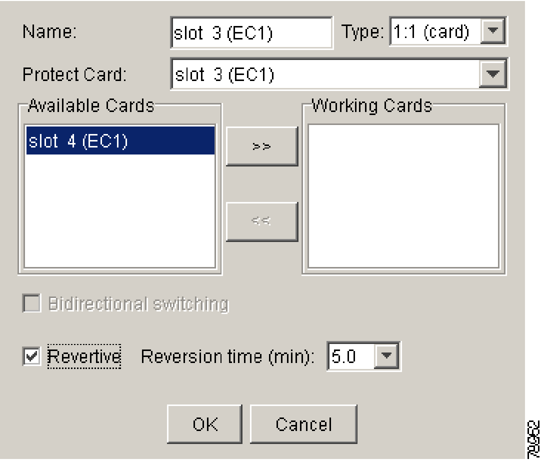
Step 3 Under Protection Groups, click **Create**.

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 characters.
- *Type*—Choose 1:1 from the pull-down menu.
- *Protect Card*—Choose the protect card from the pull-down menu. The menu displays cards available for 1:1 protection. If no cards are available, no cards are displayed.

After you choose the protect card, a list of cards available for protection is displayed under Available Cards, as shown in Figure 4-9. If no cards are available, no cards are displayed. If this occurs, you can not complete this task until you install the physical cards or pre-provision the ONS 15454 slots.

Figure 4-9 Creating a 1:1 protection group



Name: slot 3 (EC1) Type: 1:1 (card)

Protect Card: slot 3 (EC1)

Available Cards: slot 4 (EC1)

Working Cards:

□ Bidirectional switching

☑ Revertive Reversion time (min): 5.0

Step 5 From the Available Cards list, choose the card that will be protected by the card selected in *Protect Card*. 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 box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time entered in *Reversion Time*.
- *Reversion time*—If *Revertive* is checked, choose the reversion time. Click the *Reversion time* field and select a reversion time from the pull-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 7 Click **OK**, then click **Yes** on the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-72 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	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
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:N requirements specified in Table 4-3 on page 4-24.

Step 2 Click the **Provisioning** > **Protection** tabs.

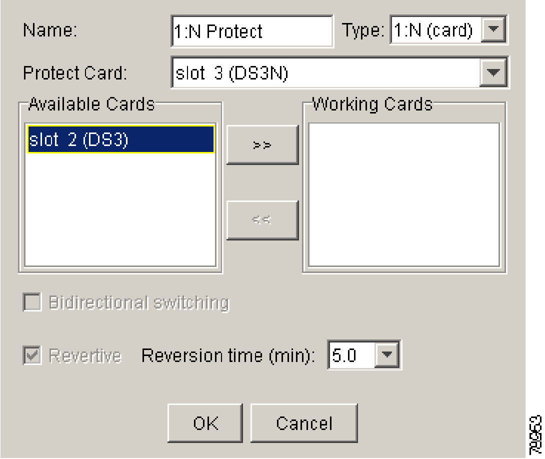
Step 3 Under Protection Groups, click **Create**.

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 characters.
- *Type*—Choose 1:N from the pull-down menu.
- *Protect Card*—Choose the protect card from the pull-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 display in the pull-down menu.

After you choose the protect card, a list of cards available for protection is displayed under Available Cards, as shown in Figure 4-10. If no cards are available, no cards are displayed. If this occurs, you will not be able to complete this task until you install the physical cards or provision the ONS 15454 slots.

Figure 4-10 Creating a 1:N protection group



Name: 1:N Protect Type: 1:N (card)

Protect Card: slot 3 (DS3N)

Available Cards: slot 2 (DS3)

Working Cards

□ Bidirectional switching

☑ Revertive Reversion time (min): 5.0

Step 5 From the Available Cards list, choose the cards that will be protected by the card selected in the Protect Card pull-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 the *Reversion time* field and select a reversion time from the pull-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 7 Click **OK**, then click **Yes** on the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-73 Create a 1+1 Protection Group

Purpose	Use this task to create a 1+1 protection group for any OC-N card/port (OC-3, OC-12, OC-12-4, OC-48, OC-48AS, and OC-192).
Tools/Equipment	Installed OC-N cards or pre-provisioned slots
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
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 4-24.

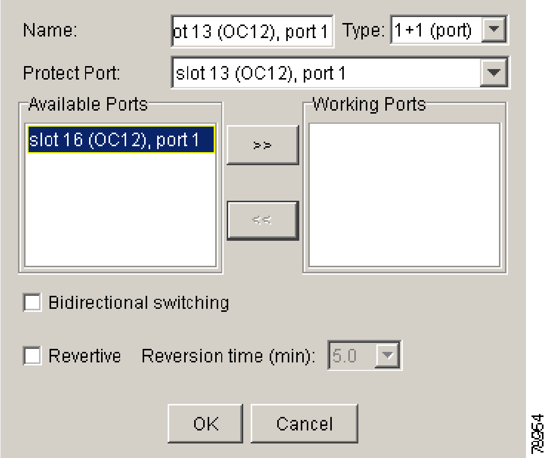
Step 2 In node view, click the **Provisioning** > **Protection** tabs.

Step 3 Under Protection Groups, 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 characters.
- *Type*—Choose 1+1 from the pull-down menu.
- *Protect Port*—Choose the protect port from the pull-down menu. The menu displays the available OC-N ports, as shown in Figure 4-11. If OC-N cards are not installed, no ports display in the pull-down menu.
- After you choose the protect port, a list of ports available for protection is displayed under Available Ports, as shown in Figure 4-11. If no cards are available, no ports are displayed. If this occurs, you will not be able to complete this task until you install the physical cards or provision the ONS 15454 slots.

Figure 4-11 Creating a 1+1 protection group



Name: pt 13 (OC12), port 1 Type: 1+1 (port)

Protect Port: slot 13 (OC12), port 1

Available Ports: slot 16 (OC12), port 1

Working Ports:

□ Bidirectional switching

□ Revertive Reversion time (min): 5.0

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:

- *Bidirectional switching*—If this box is checked, both Tx and Rx signals switch to the protect port when a failure occurs to one signal. If not checked, only the failed signal switches to the protect port.
- *Revertive*—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time entered in *Reversion Time*.
- *Reversion time*—If *Revertive* is checked, click the *Reversion time* field and select a reversion time from the pull-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-30 Create Users and Assign Security

Purpose	Use this procedure to create ONS 15454 users and assign their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Log into the ONS 15454 node where you need to create users. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

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-74 Create a New User - Single Node" task on page 4-29 and/or the "DLP-75 Create a New User - Multiple Nodes" task on page 4-30 as needed.

Note You must add the same user name and password to each node the user will access.

DLP-74 Create a New User - Single Node

Purpose	Use this task to create a new user for one ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required to add users to a node, although users can be added using TL1.
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Click the **Provisioning** > **Security** tabs.

Step 2 On the Security pane, 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 6-10 characters, and the first character must be an alpha character.
- *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 non-alphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6-10 characters, and the first character must be an alpha character. 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 The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. Each security level has a different idle time: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-75 Create a New User - Multiple Nodes

Purpose	Add a new user to multiple ONS 15454s.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu in node (default) view, choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** tabs.

Step 3 On the Security pane, 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 have no more than 10 characters, and the first character must be an alpha character.
- *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 non-alphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6-10 characters, and the first character must be an alpha character. 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 The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. Each security level has a different idle time: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

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 On the User Creation Results dialog box, click **OK**.

Step 8 Return to your originating procedure (NTP).

NTP-121 Set the Port Name for a Card

Purpose	Use this procedure to assign a name to one port on a card.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 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 the node where you want to set a port name for a card or cards. The node (default) view displays. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Double-click the card that has the port you want to provision.

Step 3 Click the **Provisioning** tab.

Step 4 Click the Name column for the port number you are naming and enter the desired port name.

The port name can be up to 32 alphanumeric/special characters and is blank by default.

Step 5 Click **Apply**.

NTP-32 Provision the Alarm Interface Controller

Purpose	Use this procedure to create external (environmental) alarms, external controls, and orderwire tunnels for the AIC card.
Tools/Equipment	An AIC card installed in Slot 9
Prerequisite Procedures	NTP-24 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-60 Log into CTC" task on page 3-22 at the node with the AIC card you want to provision.

Step 2 As needed, complete the "DLP-82 Provision External Alarms and Controls" task on page 4-32.

Step 3 As needed, complete the "DLP-83 Provision the AIC Orderwire" task on page 4-34.

Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

DLP-82 Provision External Alarms and Controls

Purpose	Use this task to provisions external alarms and controls on the AIC card.
Tools/Equipment	An AIC card must be installed in Slot 9.
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For information about the AIC external controls, virtual wire and orderwire, refer to the *Cisco ONS 15454 Reference Guide*.

Step 1 Verify the backplane wiring. See the " NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-35 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 the external relays are wired to the ENVIR ALARMS OUT backplane pins.

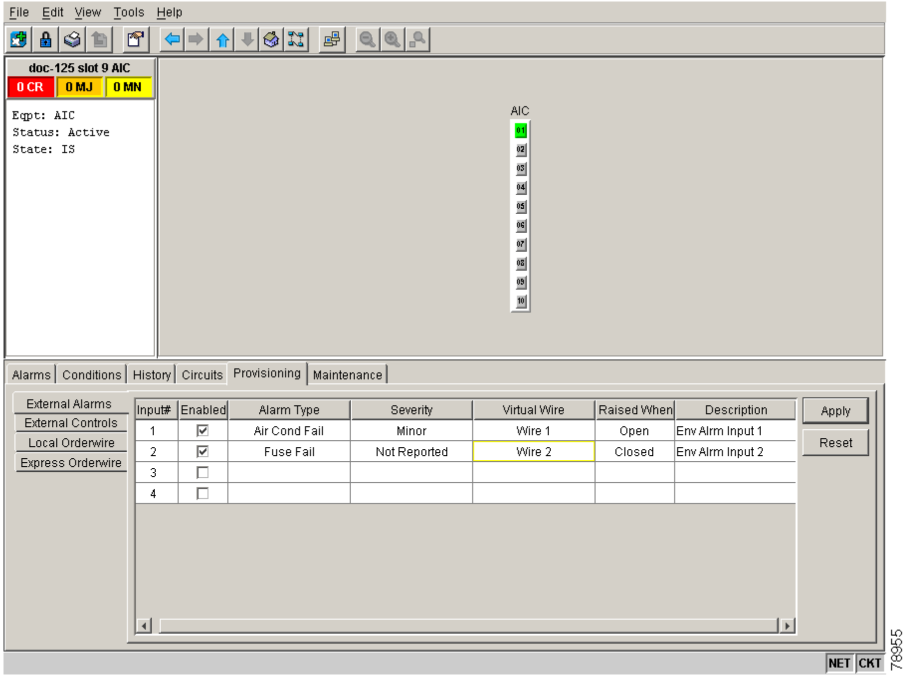
Step 2 Double-click the AIC card on the CTC shelf graphic. The card view displays.

Step 3 If you are provisioning external alarms, click the **Provisioning > External Alarms** tabs (Figure 4-12). If you are not provisioning external alarms, skip Steps 4–6 and go to Step 7.

Step 4 Complete the following fields for each external device wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.
- *Alarm Type*—Choose an alarm type from the provided list.
- *Severity*—Choose a severity. The severity determines how the alarm is displayed in the CTC Alarms and History tabs and whether the LEDs are activated. Critical, Major, and Minor activate the appropriate LEDs. Not Alarmed and Not Reported do not activate LEDs, but do report the information in CTC.
- *Virtual Wire*—To assign the external device to a virtual wire, choose the virtual wire. Otherwise, do not change the None default. For information about the AIC virtual wire, see the *Cisco ONS 15454 Reference Guide*.
- *Raised When*—Choose the contact condition (open or closed) that will trigger the alarm in CTC.
- *Description*—Default descriptions are provided for each alarm type; you can enter a different description if needed.

Figure 4-12 Provisioning external alarms on the AIC card



Eqpt: AIC
Status: Active
State: IS

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	☑	Air Cond Fail	Minor	Wire 1	Open	Env Alrm Input 1
2	☑	Fuse Fail	Not Reported	Wire 2	Closed	Env Alrm Input 2
3	□					
4	□					

Step 5 To provision additional devices, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Step 7 If you are provisioning external controls, click the **External Controls** subtab, complete the following fields for each external control wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.
- *Control Type*—Choose the control type: 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 8 To provision additional controls, complete Step 7 for each additional device.

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-83 Provision the AIC Orderwire

Purpose	Use this task to provision orderwire on the AIC card.
Tools/Equipment	An AIC card must be installed in Slot 9.
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the network view (from the View menu in node view click **Go to Network View**).

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click **Create**.

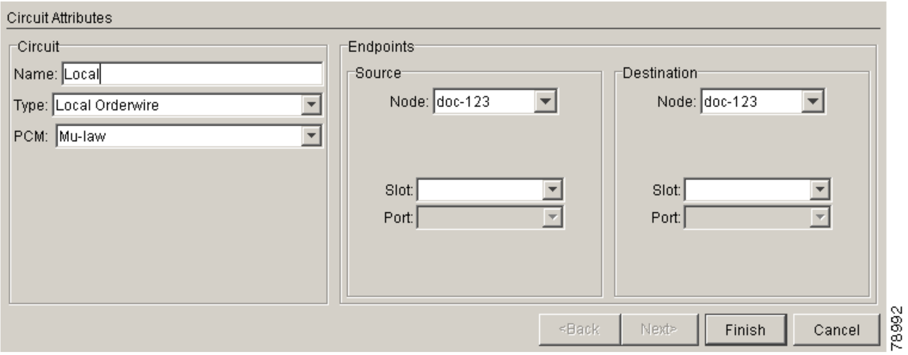
Step 4 In the Circuit Creation dialog box, complete the following fields:

- *Name*—Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces).
- *Type*—Choose either LOW (local orderwire) or EOW (express orderwire) appropriate to the orderwire path that you want to create. If regenerators are not used between ONS 15454 nodes, you can use either local or express AIC 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 either MU_LAW or A_LAW.

The Local Orderwire subtab is shown in Figure 4-13. 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.

Figure 4-13 Provisioning local orderwire



Circuit Attributes

Circuit
Name: Local
Type: Local Orderwire
PCM: Mu-law

Endpoints
Source
Node: doc-123
Slot:
Port:

Destination
Node: doc-123
Slot:
Port:

Step 5 Under Endpoints, choose the source and destination nodes and source and destination optical ports and slots from the drop-down menus.

Step 6 Click **Finish**.

Step 7 Return to your originating procedure (NTP).

NTP-123 Provision the Alarm Interface Controller-International

Purpose	Use this procedure to create external (environmental) alarms, external controls, orderwire tunnels, extension type, or station number for the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9
Prerequisite Procedures	NTP-24 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 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 AIC-I alarm contacts cannot be used. Only the AEP alarm contacts can be used. For further information about the AEP, see " NTP-119 Install the Alarm Expansion Panel" procedure on page 1-31 and the " NTP-120 Install an External Wire-Wrap Panel to the AEP" procedure on page 1-42.

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22 at the node with the AIC-I card you want to provision.

Step 2 As needed, complete the "DLP-82 Provision External Alarms and Controls" task on page 4-32.

Step 3 As needed, complete the "DLP-83 Provision the AIC Orderwire" task on page 4-34.

Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

DLP-211 Provision External Alarms and Controls on the AIC-I Card

Purpose	Use this task to provision external alarms and controls on the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	NTP-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For information about the AIC-I external controls, virtual wire, and orderwire, refer to the *Cisco ONS 15454 Reference Guide*.

Step 1 Verify the backplane wiring. If you are using the Alarm Extension Panel (AEP), see the " NTP-119 Install the Alarm Expansion Panel" procedure on page 1-31. Otherwise, see the " NTP-8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections" procedure on page 1-35 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 the external device relays are wired to the ENVIR ALARMS OUT backplane pins.

Step 2 Double-click the AIC-I card on the CTC shelf graphic. The card view displays.

Step 3 Click the **Provisioning > Card** tabs and complete the following fields for the card:

- *Add Extension*—Check this box if you are using the Alarm Extension Panel (AEP).
- *Extension Type*—Select AEP if you checked the Add Extension box.
- *Input/Output*—Select *External Alarm* if you use external alarms only; select *External Control* if you use both external alarms and external controls. Selecting only *External Alarm* gives you 16 external alarm ports and no external control ports. If you select *External Control,* four of the ports are converted to external control ports, leaving you with 12 external alarm ports.
- *Station Number*—Enter a four-digit number unique to the node. This is the orderwire "phone number" for this node. The station number is used to call this node over the orderwire channel.
- The default is 0000 and cannot be deleted. It is considered the "party line" and calls all nodes on the network when dialed.

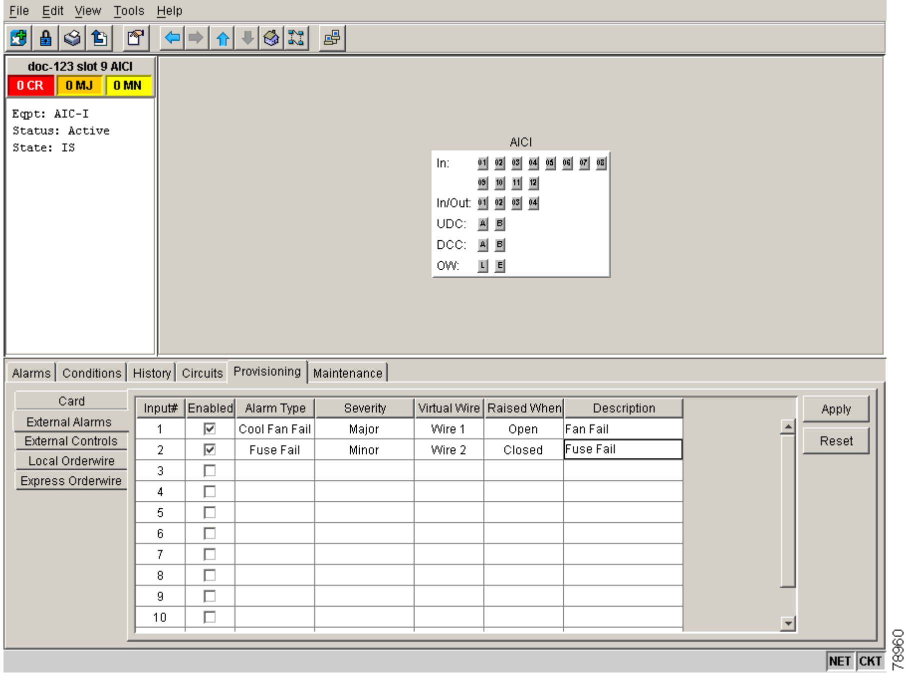
Step 4 If you are provisioning external alarms, click the **External Alarms** tab (Figure 4-14 on page 4-37). If you are not provisioning external alarms, skip Steps 5–7 and go to Step 8.

Step 5 Complete the following fields for each external device wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.
- *Alarm Type*—Choose an alarm type from the provided list.
- *Severity*—Choose a severity. The severity determines how the alarm is displayed in the CTC Alarms and History tabs and whether the LEDs are activated. Critical, Major, and Minor activate the appropriate LEDs. Not Alarmed and Not Reported do not activate LEDs, but do report the information in CTC.

- *Virtual Wire*—To assign the external device to a virtual wire, choose the virtual wire. Otherwise, do not change the None default. For information about the AIC virtual wire, see the *Cisco ONS 15454 Reference Guide*.
- *Raised When*—Choose the contact condition (open or closed) that will trigger the alarm in CTC.
- *Description*—Default descriptions are provided for each alarm type; you can enter a different description if needed.

Figure 4-14 Provisioning external alarms on the AIC-I card



Eqpt: AIC-I
Status: Active
State: IS

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	☑	Cool Fan Fail	Major	Wire 1	Open	Fan Fail
2	☑	Fuse Fail	Minor	Wire 2	Closed	Fuse Fail
3	☐					
4	☐					
5	☐					
6	☐					
7	☐					
8	☐					
9	☐					
10	☐					

Step 6 To provision additional devices, complete Step 5 for each additional device.

Step 7 Click **Apply**.

Step 8 If you are provisioning external controls, click the **External Controls** subtab and complete the following fields for each external control wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.
- *Control Type*—Choose the control type: 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 controls, complete Step 8 for each additional device.

Step 10 Click **Apply**.

Step 11 Return to your originating procedure (NTP).

DLP-212 Create a User Data Channel Circuit

Purpose	Use this task to create 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-24 Verify Card Installation, page 4-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the network view (from the View menu in node view click **Go to Network View**).

Step 2 Click the **Provisioning > Overhead Circuits** tabs.

Step 3 Click **Create**.

Step 4 In the Circuit Creation dialog box, complete the following fields:

- *Name*—Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces).
- *Type*—Choose either User Data-F1 or User Data D-4-D-12 from the drop-down menu.

Step 5 Under Endpoints, choose the source and destination nodes and source and destination optical ports and slots from the drop-down menus.

Step 6 Click **Finish**.

Step 7 Return to your originating procedure (NTP).

NTP-33 Set Up SNMP

Purpose	Sets parameters so that you can use SNMP management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-24 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 Log into the ONS 15454 node where you want to set up SNMP. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Click the **Provisioning** > **SNMP** tabs.

Step 3 Click the **Create** button. The SNMP Traps Destination dialog box appears (Figure 4-15 on page 4-39).

Step 4 On the Create SNMP Traps Destination dialog box, complete the following:

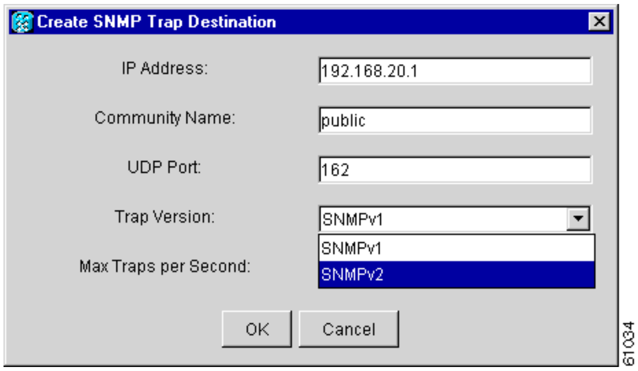
- *IP Address*—Type the IP address of your network management system. If the node you are logged into is an ENE, set the destination address to the GNE.
- *Community Name*—Type the SNMP community name. For a description of SNMP community names, refer to the SNMP information in the *Cisco ONS 15454 Reference 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 NMS.

- *UDP Port*—The default 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.
- *Trap Version*—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMP v1 or v2.
- *Max Traps per Second*—Type the maximum traps per second. The default is 0.

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.

Figure 4-15 Setting SNMP


Create SNMP Trap Destination

IP Address: 192.168.20.1

Community Name: public

UDP Port: 162

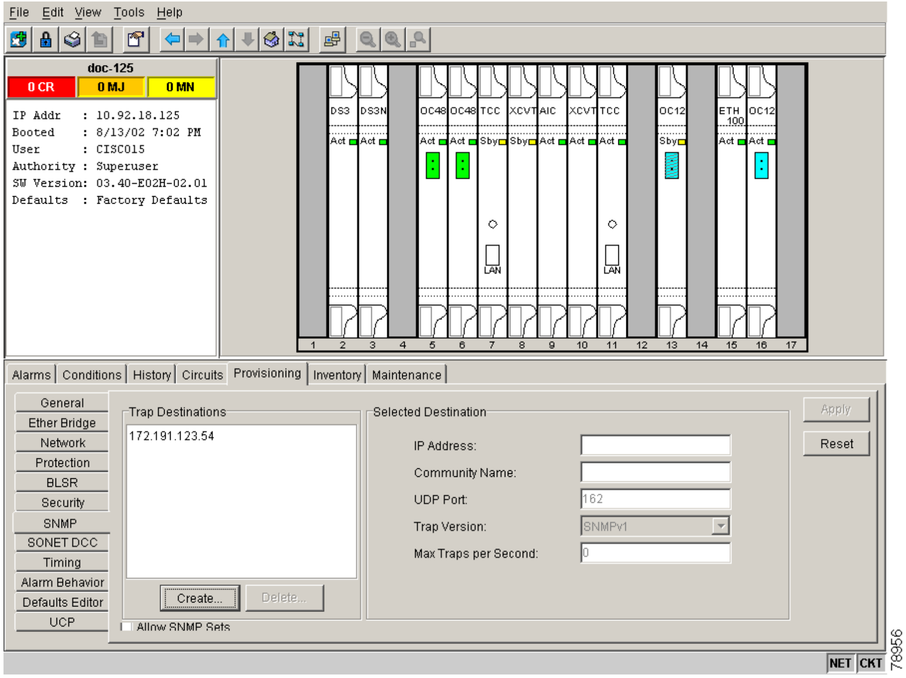
Trap Version: SNMPv1

Max Traps per Second:

Step 5 Click **OK**. Figure 4-16 on page 4-40 appears.

Step 6 Click the node IP address under Trap Destinations. Verify the SNMP information that displays under Selected Destination.

Figure 4-16 SNMP Trap Destinations



File Edit View Tools Help
doc-125
0 CR
0 MJ
0 MN

```
IP Addr   : 10.92.18.125
Booted    : 8/13/02 7:02 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

DS3 DS3N OC48 OC48 TCC XCVT AIC XCVT TCC OC12 ETH 100 OC12
Act Act Act Act Sby Sby Act Act Act Sby Act Act
LAN LAN
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Alarms Conditions History Circuits Provisioning Inventory Maintenance
General Ether Bridge Network Protection BLSR Security SNMP SONET DCC Timing Alarm Behavior Defaults Editor UCP
Trap Destinations
Selected Destination
Apply
Reset
Create...
Delete...
NET CKT
78956

Trap Destinations: 172.191.123.54

IP Address:
Community Name:
UDP Port: 162
Trap Version: SNMPv1
Max Traps per Second: 0

□ Allow SNMP Sets

NTP-34 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-24 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

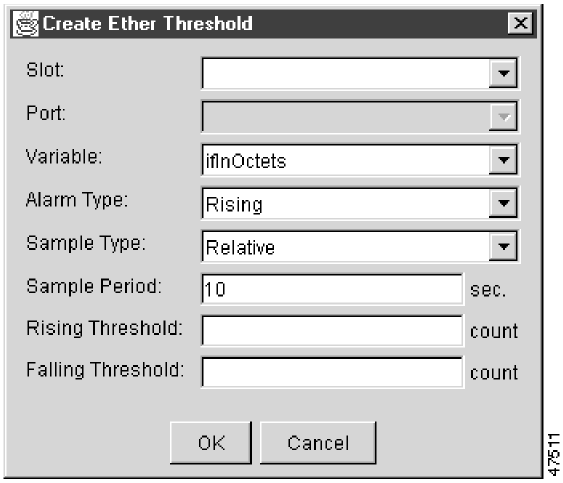
Step 1 Log into the ONS 15454 node where you want to set up SNMP. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Click the **Provisioning** > **Ether Bridge** > **Thresholds** tabs.

Step 3 Click **Create**.

The Create Ether Threshold dialog box (Figure 4-17) opens.

Figure 4-17 Creating RMON thresholds



Create Ether Threshold

Slot:

Port:

Variable: ifInOctets

Alarm Type: Rising

Sample Type: Relative

Sample Period: 10 sec.

Rising Threshold: count

Falling Threshold: count

Step 4 From the Slot menu, choose the appropriate Ethernet card.

Step 5 From the Port menu, choose the applicable port on the Ethernet card you selected.

Step 6 From the Variable menu, choose the variable. See Table 4-4 on page 4-42 for a list of the Ethernet threshold variables available in this field.

Step 7 From Alarm Type, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 From the Sample Type pull-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 any time period.

Step 9 Type in an appropriate number of seconds for the Sample Period.

Step 10 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, these occurrences fire an alarm.

Step 11 Type in the appropriate number of occurrences for the Falling Threshold. 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 12 Click **OK** to complete the procedure.

Table 4-4 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	Number of multicast frames received error free
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
ifInDiscards	The number of inbound packets which 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	Number of multicast frames transmitted error free
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent
ifOutDiscards	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, i.e., 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, i.e., there is an integral number of octets, but an incorrect Frame Check Sequence (FCS)
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollision	Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors	The number of transmission errors on a particular interface that are not otherwise counted

Table 4-4 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsJabbers	Total number of Octets of data (including bad packets) received on the network
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 – 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 – 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 – 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 – 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 – 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 802.x pause frames
transmitPauseFrames (G series only)	The number of transmitted 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

Turn Up Network

This chapter explains how to turn up and test Cisco ONS 15454s network, including point-to-point networks, linear add drop multiplexers (ADMs), unidirectional path switched rings (UPSRs), and bidirectional line switched rings (BLSRs).

Before You Begin

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

1. NTP-35 Verify Node Turn Up, page 5-2—Complete this procedure before beginning network turn up.
2. NTP-124 Provision a Point-to-Point Network, page 5-3—Complete as needed.
3. NTP-125 Point-to-Point Network Acceptance Test, page 5-6—Complete this procedure after you provision a point-to-point network.
4. NTP-38 Provision a Linear ADM Network, page 5-13—Complete as needed.
5. NTP-39 Linear ADM Network Acceptance Test, page 5-14—Complete this procedure after you provision a linear ADM.
6. NTP-40 Provision BLSR Nodes, page 5-16—Complete this procedure to provision ONS 15454s in a two-fiber or four-fiber BLSR.
7. NTP-126 Create a BLSR, page 5-19—Complete this procedure after provisioning the BLSR nodes.
8. NTP-42 Two-Fiber BLSR Acceptance Test, page 5-21—Complete this procedure after you provision a two-fiber BLSR.
9. NTP-43 Four-Fiber BLSR Acceptance Test, page 5-26—Complete this procedure after you provision a four-fiber BLSR.
10. NTP-44 Provision UPSR Nodes, page 5-31—Complete as needed.
11. NTP-45 UPSR Acceptance Test, page 5-33—Complete this procedure after you provision a UPSR.
12. NTP-46 Subtend a UPSR from a BLSR, page 5-36—Complete as needed.
13. NTP-47 Subtend a BLSR from a UPSR, page 5-37—Complete as needed.
14. NTP-48 Subtend a BLSR from a BLSR, page 5-37—Complete as needed.
15. NTP-49 Create a DCC Tunnel, page 5-40—Complete as needed.

NTP-35 Verify Node Turn Up

Purpose	Use this procedure to verify that each ONS 15454 is ready for network turn up before adding nodes 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 Log into an ONS 15454 on the network you will test. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If alarms are displayed, 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 displayed 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 on the CD. Follow the upgrade procedures appropriate to the software currently installed on the node.
- If the node defaults are not correct, complete the "NTP-165 Import Network Element Defaults" procedure on page C-3.

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-81 Change Node Management Information" procedure on page 10-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that timing settings match the settings of your site plan. If not, see the "NTP-85 Change Node Timing" procedure on page 10-20.

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-82 Change CTC Network Access" procedure on page 10-4.

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-84 Modify or Delete Card Protection Settings" procedure on page 10-14.

Step 8 Click the **Provisioning > Security** tabs. Verify that all users have been created and their security levels match the settings indicated by your site plan. If not, see the "NTP-86 Modify Users and Change Security" procedure on page 10-22.

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-87 Change SNMP Settings" procedure on page 10-26.

Step 10 Provision the network using the applicable procedure on page 5-1.

NTP-124 Provision a Point-to-Point Network

Purpose	Use this procedure to provision two ONS 15454s in a point-to-point (terminal) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-35 Verify Node Turn Up, page 5-2
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the network where you want to provision a point-to-point configuration. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards. Complete the "DLP-73 Create a 1+1 Protection Group" task on page 4-27 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 shown in CTC is connected to the working card in the other node, and that the protect card shown in CTC is connected to the protect card in the other node.

Step 5 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for the working OC-N card/port on both point-to-point nodes.

Note DCC terminations are not provisioned on the protect cards/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 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 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-28 Set Up Timing" procedure on page 4-18 for one or both of the nodes. If a node uses line timing, make its working OC-N the timing source.

Step 7 Complete the "NTP-125 Point-to-Point Network Acceptance Test" procedure on page 5-6.

DLP-213 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-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node (login) view.

Step 2 Click the **Provisioning > SONET DCC** tabs.

Step 3 Click **Create**.

Step 4 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.

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 "NTP-49 Create a DCC Tunnel" procedure on page 5-40.

Step 5 Under Port State, click the **Set to IS, if allowed** radio button.

Step 6 Verify the Disable OSPF on DCC Link checkbox is unchecked.

Step 7 Click **OK**.

Note EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms are displayed until you create all network DCC terminations and put the DCC termination OC-N ports in service.

Step 8 Return to your originating procedure (NTP).

DLP-214 Change the Service State for a Port

Purpose	Use this task to put a port in service or to remove a port from service.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To provision Ethernet ports, see the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73 or the "DLP-222 Provision G1000-4 Ethernet Ports" task on page 6-82.

Step 1 Display the node (login) view.

Step 2 On the shelf graphic, double-click the card with the port(s) you want to put in or out of service. The card view displays.

Step 3 Click the **Provisioning** > **Line** tabs.

Step 4 Under State, 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 it 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, it suppresses alarms and conditions and allows loopbacks to be performed on the port. 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; traffic alarms are suppressed and loopbacks can be performed until a signal is received for the time specified in AINS Soak, after which the state is changed to IS.

Step 5 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 state will stay in OOS-AINS state after the signal is continuously received.

Step 6 Click **Apply**.

Step 7 As needed, repeat this task for each port.

Step 8 Return to your originating procedure (NTP).

NTP-125 Point-to-Point Network Acceptance Test

Purpose	Use this procedure to test a point-to-point ONS 15454 network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-124 Provision a Point-to-Point Network, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into one of the point-to-point nodes. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Export the alarm data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 5 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Export the conditions data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 7 On the network map, double-click one point-to-point node to display it in node view.

Step 8 Create a test circuit from the login node to the other point-to-point node:

- For DS-1 circuits, complete the "NTP-128 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.
- For DS-3 circuits, complete the "NTP-131 Create an Automatically Routed DS-3 Circuit" procedure on page 6-17. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

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. After you choose muxed DS-3, choose the DS-1 to test on the muxed DS-3. 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 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 11.

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); attach the other end to the port's receive (Rx).

Step 12 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 13 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 8–12 to make sure the test set and cabling is configured correctly.

Step 14 Inject BIT errors from the test set. Verify that the errors display at the test set, indicating a complete end-to-end circuit.

Step 15 Complete the "DLP-215 TCC+ Active/Standby Switch Test" task on page 5-8.

Step 16 Complete the "DLP-216 Cross-Connect Card Active/Standby Switch Test" task on page 5-10.

Step 17 Complete the "DLP-88 Optical 1+1 Protection Test" task on page 5-12.

Step 18 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 19 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 20 From the View menu, choose **Go to Network View**.

Step 21 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 22 Export the Alarms data to a file.

Step 23 Repeat Steps 11–22 for the other point-to-point node.

Step 24 If a node fails any test, repeat the test verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 25 Delete the test circuit. See the "NTP-152 Delete Circuits" procedure on page 9-11 for instructions.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

DLP-215 TCC+ Active/Standby Switch Test

Purpose	This task verifies that the ONS 15454 TCC+ 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-60 Log into CTC, page 3-22
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. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

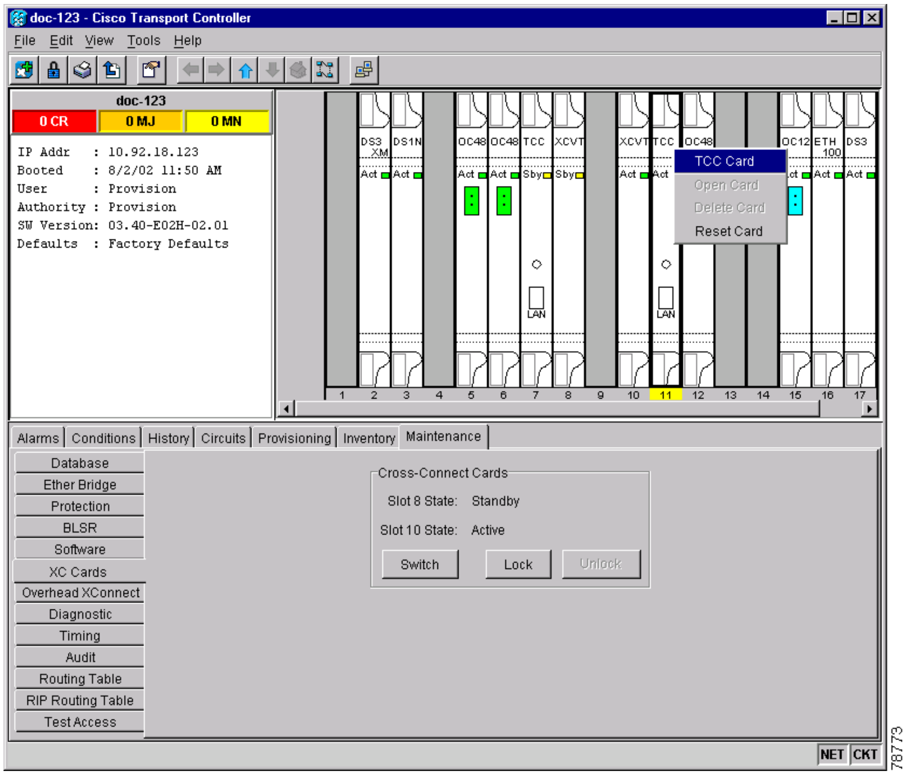
Step 3 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the Cisco ONS 15454 Troubleshooting Guide.

Step 4 Display the node containing the TCC+s you are testing in node view.

Step 5 Make a note of which TCC+ is active and which is standby by examining the LEDs on the shelf graphic. TCC+ cards are installed in Slot 7 and Slot 11. The active TCC+ has a green ACT LED, and the standby TCC+ has an amber SBY LED.

Step 6 On the shelf graphic, right-click the active TCC+ and choose **Reset** from the shortcut menu (Figure 5-1).

Figure 5-1 Resetting the active TCC+



doc-123 - Cisco Transport Controller

```
IP Addr   : 10.92.18.123
Booted    : 8/2/02 11:50 AM
User      : Provision
Authority : Provision
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Cross-Connect Cards

Slot 8 State: Standby

Slot 10 State: Active

Step 7 On the Resetting Card dialog box, click **Yes**. After 20-40 seconds, a "lost node connection, changing to network view" message is displayed.

Step 8 Click **OK**. On the network view map, the node where you reset the TCC+ will be grey.

Step 9 After the node icon turns green (within 1-2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby TCC+ displays a green ACT LED.
- The previous active TCC+ LEDs will go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (TCC+ is in standby mode). The LEDs should complete this sequence within 5-10 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– 10 to return the active/standby TCC+s to their configuration at the start of the procedure.

Step 12 Verify that the TCC+ card's display is the same as noted in Step 1.

Step 13 Return to your originating procedure (NTP).

DLP-216 Cross-Connect Card Active/Standby Switch Test

Purpose	This task verifies that the ONS 15454, 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-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

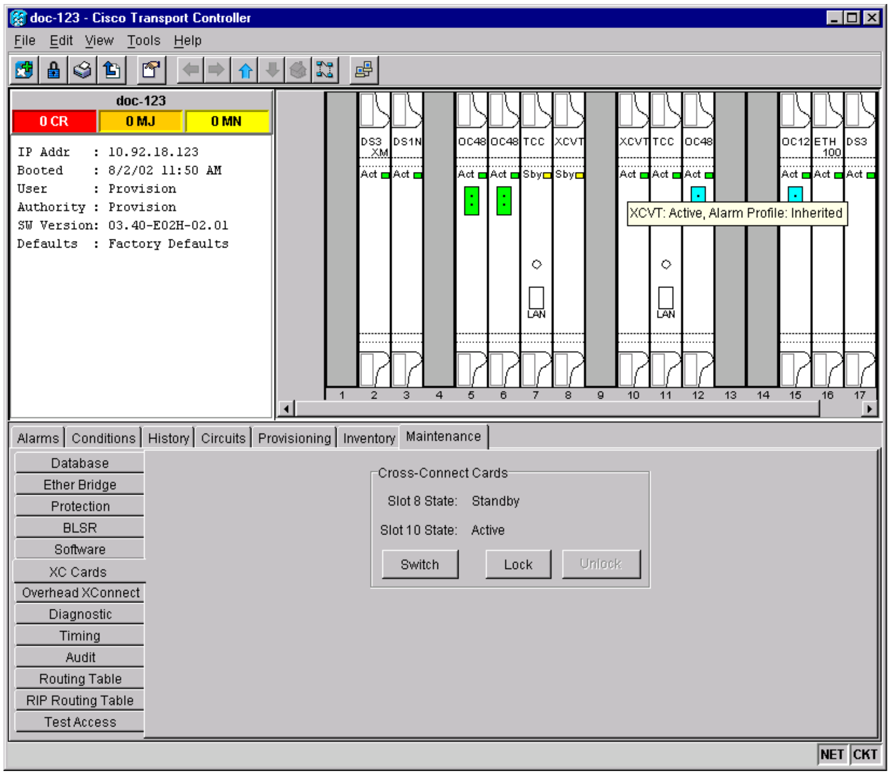
Step 2 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Display the node containing the cross-connect cards you are testing in node view.

Step 5 Click the **Maintenance > XC Cards** tabs (Figure 5-2).

Figure 5-2 Performing a cross-connect card switch



```
IP Addr   : 10.92.18.123
Booted    : 8/2/02 11:50 AM
User      : Provision
Authority : Provision
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Cross-Connect Cards

Slot 8 State: Standby

Slot 10 State: Active

Step 6 Under Cross-Connect Cards, make a note of the active and standby slots.

Step 7 On the shelf graphic, verify that the active cross-connect card displays a green ACT LED and the standby cross-connect card displays an amber SBY LED. If these conditions are not present, review the "DLP-37 Install the XC, XCVT, or XC10G Cards" task on page 2-8 or contact your next level of support.

Step 8 Click the **Switch** button.

Step 9 On 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 display within 1-2 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 Repeat Steps 7–9 to return the active/standby slots to their configuration at the start of the procedure.

Step 13 Verify that the cross-connect card display is the same as noted in Step 6.

Step 14 Return to your originating procedure (NTP).

DLP-88 Optical 1+1 Protection Test

Purpose	This task verifies a 1+1 protection group will switch traffic properly.
Tools/Equipment	The test set specified by the acceptance test procedure
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22; 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. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Display the node containing the 1+1 protection group you are testing in node view.

Step 5 Click the **Maintenance > Protection** tabs.

Step 6 Under Protection Groups, click the 1+1 protection group.

Step 7 Click the working port and click the **Force Switch Command** button.

Step 8 At the Confirm Manual Operation dialog, click **Yes**.

Step 9 Under Selected Group, verify that the following is displayed:

Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT] [PORT STATE]

Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 10 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 Steps 11–12, then refer to your next level of support.

Step 11 Click the **Clear Switch Command** button.

Step 12 At the Confirm Clear Operation confirmation, click **Yes**.

Step 13 Under Selected Group, click the protect port and then click the **Force Switch Command** button.

Step 14 At the Confirm Force Operation popup window, click **Yes**.

Step 15 Under Selected Group, verify that the following is displayed:

Protect port - Protect/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Working port - Working/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 16 Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, refer to your next level of support.

Step 17 Click the **Clear Switch Command** button.

Step 18 At the Confirm Clear Operation dialog, click **Yes**.

Step 19 Under Selected Group, verify the following states:

- Protect port - Protect/Standby
- Working port - Working/Active

Step 20 Return to your originating procedure (NTP).

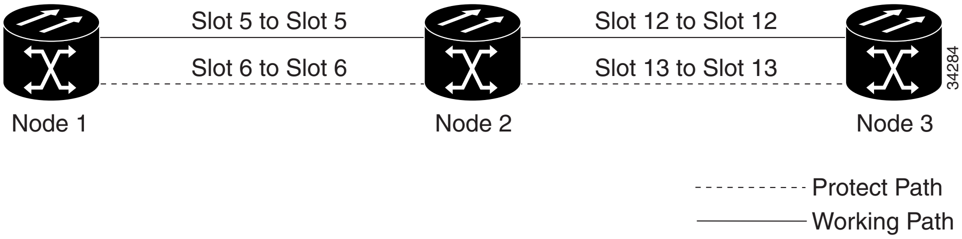
NTP-38 Provision a Linear ADM Network

Purpose	This procedure provisions three or more ONS 15454s in a linear add/drop network.
Tools/Equipment	None
Prerequisite Procedures	NTP-35 Verify Node Turn Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 that you want to provision in a linear ADM network. The node (default) view displays. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Figure 5-3 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 5-3 A 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, go to the "DLP-73 Create a 1+1 Protection Group" task on page 4-27 to create them.

Step 3 Repeat Steps 1 and 2 for all other nodes you will include in the linear ADM.

Step 4 Verify that cards set as working and protect 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-213 Provision SONET DCC Terminations" task on page 5-4 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 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 5-3) will have one DCC termination, and intermediate nodes (Node 2 in Figure 5-3) will have two DCC terminations (Slots 5 and 12 in the example).

Step 6 Verify that timing has been set up at each linear node. If not, complete the "NTP-28 Set Up Timing" task on page 4-18. If a node is using line timing, use its working OC-N card as the timing source.

Step 7 Complete the "NTP-39 Linear ADM Network Acceptance Test" procedure on page 5-14.

NTP-39 Linear ADM Network Acceptance Test

Purpose	Use this procedure to test a linear ADM network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-38 Provision a Linear ADM Network, page 5-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the linear ADM network you are testing. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Export the alarm data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. Complete the "DLP-139 Export CTC Data" task on page 7-3.

Step 5 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Export the conditions data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 7 Display a linear ADM node in node view.

Step 8 Create a test circuit from that node to an adjacent linear ADM node.

- For DS-1 circuits, complete the "NTP-128 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

- For DS-3 circuits, complete the "NTP-131 Create an Automatically Routed DS-3 Circuit" procedure on page 6-17. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

Step 9 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. After you choose muxed DS-3, choose the DS-1 to test on the muxed DS-3. 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 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 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 destination 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 displays a clean signal. If a clean signal is not displayed, repeat Steps 8–12 to make sure the test set and cabling is configured correctly.

Step 14 Inject BIT errors from the test set. Verify that the errors display at the test set, indicating a complete end-to-end circuit.

Step 15 Complete the "DLP-215 TCC+ Active/Standby Switch Test" task on page 5-8.

Step 16 Complete the "DLP-216 Cross-Connect Card Active/Standby Switch Test" task on page 5-10.

Step 17 Complete the "DLP-88 Optical 1+1 Protection Test" task on page 5-12 to test the OC-N port protection group switching.

Step 18 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 19 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 20 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 21 Delete the test circuit. See the "NTP-152 Delete Circuits" procedure on page 9-11 for instructions.

Step 22 Display the next linear ADM node in node view and repeat Steps 8–21.

Step 23 If a node fails any test, repeat the test 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.

NTP-40 Provision BLSR Nodes

Purpose	This procedure provisions ONS 15454 nodes for a bidirectional line switched ring.
Tools/Equipment	None
Prerequisite Procedures	NTP-35 Verify Node Turn Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-44 Install Fiber-Optic Cables for BLSR Configurations" task on page 2-26, 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 5-4. In the figure, the OC-N line card on the left side of the shelf is the west port, and the line card on the right side of the shelf is considered the east port.
- 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 5-5. 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 5-4 ***Four-node, two-fiber BLSR fiber connection example***

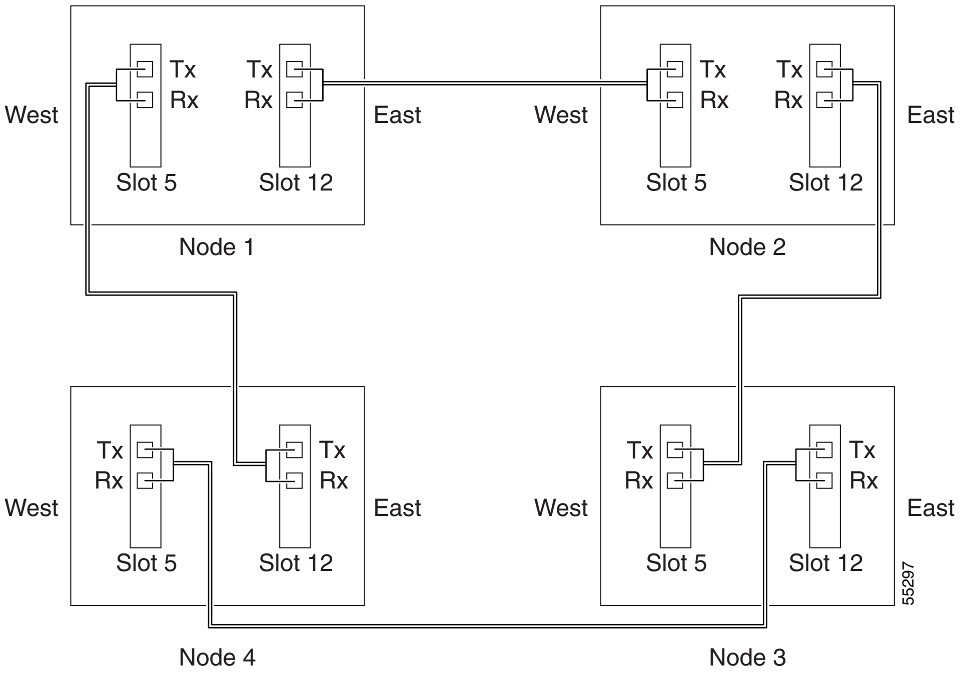
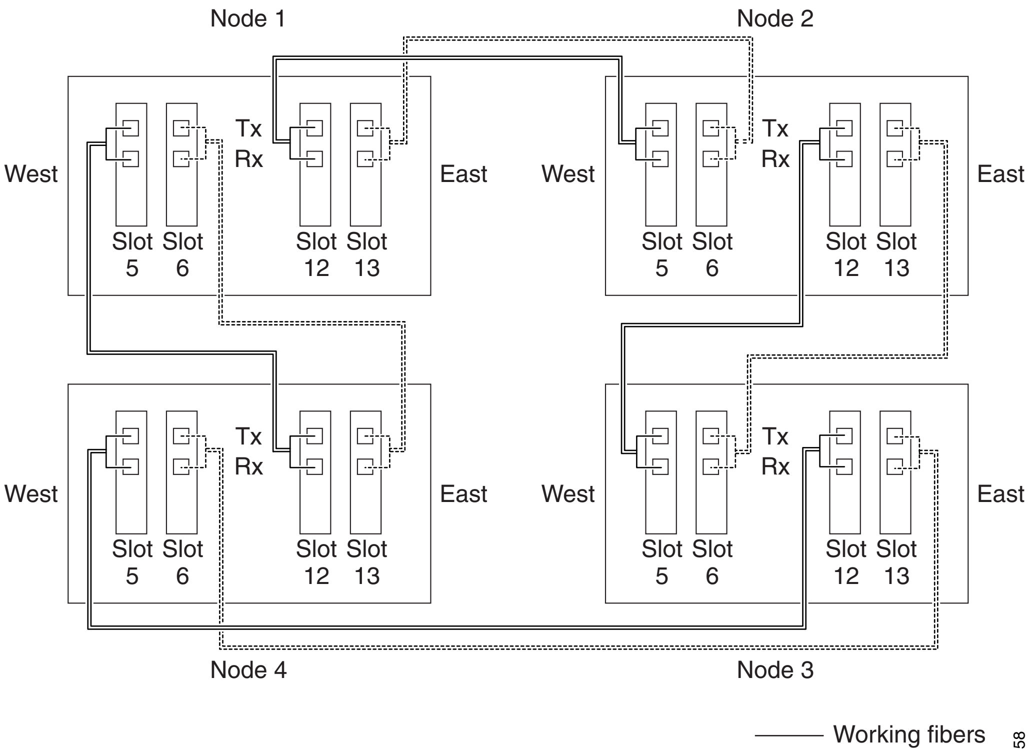


Figure 5-5 ***Four-node, four-fiber BLSR fiber connection example***



Step 2 Log into an ONS 15454 that you want to configure in a BLSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 3 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4. 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 not the protect cards.

Note If an ONS 15454 is not connected to a corporate LAN, DCC provisioning must be performed through a local craft connection to the node. Remote provisioning is possible only after all nodes in the network have DCC provisioned to in-service OC-N ports.

Step 4 For four-fiber BLSRs, complete the "DLP-214 Change the Service State for a Port" task on page 5-5 for the protect OC-N ports.

Step 5 If a BLSR span passes through third-party equipment that cannot transparently transport the K3 byte, complete the "DLP-89 Remap the K3 Byte" task on page 5-18. This task is not necessary for most users.

Step 6 Repeat Steps 2–4 at each node that will be in the BLSR.

Step 7 Complete the "NTP-126 Create a BLSR" procedure on page 5-19.

DLP-89 Remap the K3 Byte

Purpose	Use this task to provision 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	NTP-35 Verify Node Turn Up, page 5-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
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 At the 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 (Four-fiber BLSR only) Repeat Steps 2–4 for each protect card.

Step 6 Repeat Steps 2–4 at the node and card on the other end of the BLSR span.

Step 7 Return to your originating procedure (NTP).

NTP-126 Create a BLSR

Purpose	This procedure creates a BLSR at each BLSR-provisioned node.
Tools/Equipment	None
Prerequisite Procedures	NTP-40 Provision BLSR Nodes, page 5-16
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 node on the network where you will create the BLSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click **Create BLSR**.

Step 5 On the BLSR Creation dialog box (Figure 5-6), 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, OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk 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 ID*—Assign a ring ID (a number between 0 and 9999).
- *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.

Figure 5-6 Setting BLSR properties

Step 6 Click **Next**. If CTC displays a network graphic, go to the next step. If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with UPSR selectors, a Cannot Create BLSR message is displayed. If this occurs, complete the following steps:

a. Click **OK**.

b. On 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-40 Provision BLSR Nodes" procedure on page 5-16, making sure all steps are completed accurately, then start this procedure again.

Step 7 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards comprising a complete ring, the lines turn blue and the Finish button is displayed. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC conected, go to Step 8 if you are completing a 4-fiber BLSR or go to Step 9 if you are completing a 2-fiber BLSR).

Step 8 (4 Fiber BLSRs only) Click **Next**. In the Protect Port Selection section, choose the protect ports from the West Protect and East Protect columns, go to the next step.

Step 9 Click **Finish**. If CTC displays the BLSR window with the BLSR you created, go to Step 10. If CTC displays a Cannot Create BLSR or Error While Creating BLSR message:

a. Click **OK**.

b. On 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-40 Provision BLSR Nodes" procedure on page 5-16, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms may briefly display during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, BLSROSYNC.

Step 10 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.

Step 11 Complete the "NTP-42 Two-Fiber BLSR Acceptance Test" procedure on page 5-21 or the "NTP-43 Four-Fiber BLSR Acceptance Test" procedure on page 5-26.

NTP-42 Two-Fiber BLSR Acceptance Test

Purpose	This procedure tests a two-fiber ONS 15454 BLSR.
Tools/Equipment	Test set and cables appropriate for the test circuit
Prerequisite Procedures	NTP-40 Provision BLSR Nodes, page 5-16
	NTP-126 Create a BLSR, page 5-19
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform span 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 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 Log into one of the ONS 15454s on the BLSR you are testing. (This node will be called Node 1.) See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Export the alarms data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 5 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Export the conditions data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 7 On the network view, double-click Node 1.

Step 8 Complete the "DLP-217 BLSR Exercise Ring Test" task on page 5-23.

Step 9 Create a test circuit from Node 1 to the node connected to the East OC-N trunk card of Node 1. (This node will be called Node 2.)

- For DS-1 circuits, complete the "NTP-128 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

- For DS-3 circuits, complete the "NTP-131 Create an Automatically Routed DS-3 Circuit" procedure on page 6-17. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

Step 10 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. After you choose muxed DS-3, choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.

Step 11 Verify the integrity of all patch cables that will be used in this test by connecting the test set transmit (Tx) the test set receive (Rx). 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 12 Create a physical loopback at the circuit destination card: attach one end of a patch cable to the destination port's transmit (Tx); attach the other end to the port's receive (Rx).

Step 13 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 14 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 1–13 to make sure the test set and cabling is configured correctly.

Step 15 Inject BIT errors from the test set. Verify that the errors display at the test set, verifying a complete end-to-end circuit.

Step 16 Complete the "DLP-215 TCC+ Active/Standby Switch Test" task on page 5-8.

Step 17 Complete the "DLP-216 Cross-Connect Card Active/Standby Switch Test" task on page 5-10.

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 18 Complete the "DLP-91 BLSR Ring Switch Test" task on page 5-24 at Node 1.

Step 19 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 20 Complete the "NTP-152 Delete Circuits" procedure on page 9-11 for the test circuit.

Step 21 Repeating steps 7–20 for Nodes 2 and higher, work your way around the BLSR, testing each node and span in the ring. 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 If a node fails any test, repeat the test to verify 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 6, "Create Circuits and VT Tunnels."

DLP-217 BLSR Exercise Ring Test

Purpose	This task tests the BLSR ring functionality without switching traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are in card or node view, from the View menu, choose **Go to Network View**. Otherwise, go to Step 2.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the row of the BLSR you will exercise, then click **Edit**.

Step 4 Right-click the west port of any BLSR node and choose **Set West Protection Operation**. Figure 5-7 shows an example. (To move a graphic icon, click it, press **Ctrl**, and drag the icon 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 port.

Figure 5-7 Invoking a protection operation on a three-node BLSR

Step 5 On the Set West Protection Operation dialog box, choose **EXERCISE RING** from the pull-down menu. Click **OK**.

Step 6 On the Confirm BLSR Operation dialog box, click **Yes**.

On the network graphic, an E is displayed on the working BLSR channel where you invoked the protection switch. The E will display for 10-15 seconds, then disappear.

Step 7 From the File menu, choose **Close**.

Step 8 Click the **Conditions** tab, then click **Retrieve**.

Step 9 Verify that an EXERCISE-RING-REQ (Exercising Ring Request) condition is reported for the node where you exercised the ring, and an FE-EXERCISING-RING (Far End Exercising Ring) condition is reported against the far end node where you exercised the ring. Make sure the Filter button in the lower right corner of window is off (not depressed). Click the Node column to sort conditions by node.

Step 10 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 11 Return to your originating procedure (NTP).

DLP-91 BLSR Ring Switch Test

Purpose	Use this task to verify that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are in card or node view, from the View menu, choose **Go to Network View**. Otherwise, go to Step 2.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click the row of the BLSR you will switch, then click **Edit**.

Step 4 Right-click any BLSR node west port and choose **Set West Protection Operation**. Figure 5-7 on page 5-23 shows an example. (To move a graphic icon, click it, press **Ctrl**, and drag the icon 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 port.

Step 5 On the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed on the working BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the force was invoked, and all span lines between other BLSR nodes turn green.

Step 7 Click the **Conditions** tab, then click **Retrieve**.

Step 8 Verify that a RING-SW-WEST (Ring Switch West) condition is reported on the node where you invoked the force switch, and a RING-SW-EAST (Ring 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 (not depressed). Click the Node column to sort conditions by node.

Step 9 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 10 Display the BLSR window where you invoked the force ring switch (the window may be hidden by the CTC window).

Step 11 Right-click the west port of the BLSR node where you invoked the force ring switch and choose **Set West Protection Operation**.

Step 12 On the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 13 Click **Yes** on the Confirm BLSR Operation dialog box.

On the network graphic, the F indicating the force ring 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 Right-click the east port of BLSR node and choose **Set East Protection Operation**.

Step 15 On the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down menu. Click **OK**.

Step 16 Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed on the working BLSR channel where you invoked the force ring switch. The BLSR span lines are purple where the force was invoked, and all span lines between other BLSR nodes are green. The span lines may take a few moments to change color.

Step 17 Click the **Conditions** tab, then click **Retrieve**.

Step 18 Verify that a RING-SW-EAST (Ring Switch East) condition is reported on the node where you invoked the force switch, and a RING-SW-WEST (Ring Switch West) condition is reported on the node connected to the west line of the node where you performed the switch.

Step 19 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 20 Display the BLSR window where you invoked the force ring switch (the window may be hidden by the CTC window).

Step 21 Right-click the west port of the BLSR node where you invoked the force ring switch and choose **Set East Protection Operation**.

Step 22 On the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 23 Click **Yes** on the Confirm BLSR Operation dialog box.

On the network graphic, the F indicating the force ring 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 24 Close the BLSR window: from the File menu, choose **Close**.

Step 25 Return to your originating procedure (NTP).

NTP-43 Four-Fiber BLSR Acceptance Test

Purpose	This procedure tests a four-fiber ONS 15454 BLSR.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-40 Provision BLSR Nodes, page 5-16
	NTP-126 Create a BLSR, page 5-19
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform span 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 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 Log into one of the ONS 15454s on the BLSR you are testing. (This node will be called Node 1.) See the “DLP-60 Log into CTC” task on page 3-22 for instructions. The node (default) view displays.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Export the alarms data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the “DLP-139 Export CTC Data” task on page 7-3 for additional information.

Step 5 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Export the conditions data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the “DLP-139 Export CTC Data” task on page 7-3 for additional information.

Step 7 On the network map, double-click Node 1.

Step 8 Complete the “DLP-92 Four-Fiber BLSR Exercise Span Test” task on page 5-28.

Step 9 Complete the “DLP-217 BLSR Exercise Ring Test” task on page 5-23.

Step 10 Create a test circuit between Node 1 and Node 2.

- For DS-1 circuits, complete the “NTP-128 Create an Automatically Routed DS-1 Circuit” procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.
- For DS-3 circuits, complete the “NTP-131 Create an Automatically Routed DS-3 Circuit” procedure on page 6-17. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

Step 11 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. After you choose muxed DS-3, choose the DS-1 to test on the muxed DS-3. For information about configuring your test set, consult your test set user guide.

Step 12 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) and the other of the cable to the test set receive (Rx). 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 13 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 14 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 15 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 8–14 to make sure the test set and cabling is configured correctly.

Step 16 Inject global BIT errors from the test set. Verify that the errors display at the test set, verifying a complete end-to-end circuit.

Step 17 Complete the "DLP-215 TCC+ Active/Standby Switch Test" task on page 5-8.

Step 18 Complete the "DLP-216 Cross-Connect Card Active/Standby Switch Test" task on page 5-10.

Step 19 Complete the "DLP-91 BLSR Ring Switch Test" task on page 5-24 to test the BLSR protection switching at Node 1.

Step 20 Complete the "DLP-93 Four-Fiber BLSR Span Switching Test" task on page 5-29 at Node 1.

Step 21 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 22 Complete the "NTP-152 Delete Circuits" procedure on page 9-11 for the test circuit.

Step 23 At Node 2, repeat Steps 7–23, creating a test circuit between Node 2 and the node connected to the east OC-N trunk card of Node 2 (Node 3). Work your way around the BLSR creating test circuits between every two consecutive nodes.

Step 24 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 25 View Alarms and conditions on each node and record the results by exporting to a file. See the "DLP-139 Export CTC Data" task on page 7-3 for instructions.

Step 26 If a node fails any test, repeat the test 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 6, "Create Circuits and VT Tunnels."

DLP-92 Four-Fiber BLSR Exercise Span Test

Purpose	This task exercises a four-fiber BLSR span.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are in card or node view, from the View menu, choose **Go to Network View**. Otherwise, go to Step 2.

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, click it, press **Ctrl**, and drag the icon to a new location.)

Note For four-fiber BLSRs, the squares represent ports. Right-click either working port.

b. On the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the pull-down menu. Click **OK**.

c. On the Confirm BLSR Operation dialog box, click **Yes**.

On the network graphic, an E is displayed on the working BLSR channel where you invoked the protection switch. The E will display for 10-15 seconds, then disappear.

Step 5 Click the **Conditions** tab, then click **Retrieve**.

Step 6 Verify that an EXERCISE-SPAN-REQ (Exercising Span Request) condition is reported for the node where you exercised the ring, and an FE-EXERCISING-SPAN (Far End Exercising Ring) condition is reported against the far end node where you exercised the ring. Make sure the Filter button in the lower right corner of window is off (not depressed). Click the Node column to sort conditions by node.

Step 7 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 8 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. On the Set East Protection Operation dialog box, choose **EXERCISE SPAN** from the pull-down menu. Click **OK**.

c. On the Confirm BLSR Operation dialog box, click **Yes**.

On the network graphic, an E is displayed on the working BLSR channel where you invoked the protection switch. The E will display for 10-15 seconds, then disappear.

Step 9 From the File menu, choose **Close**.

Step 10 Click the **Conditions** tab, then click **Retrieve**.

Step 11 Verify that an EXERCISE-SPAN-REQ (Exercising Span Request) condition is reported for the node where you exercised the ring, and an FE-EXERCISING-SPAN (Far End Exercising Span) condition is reported against the far end node where you exercised the ring. Make sure the Filter button in the lower right corner of window is off (not depressed). Click the Node column to sort conditions by node.

Step 12 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 13 From the File menu choose **Close** to close the BLSR window..

Step 14 Return to your originating procedure (NTP).

DLP-93 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	NTP-40 Provision BLSR Nodes, page 5-16
	NTP-126 Create a BLSR, page 5-19
	DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are in card or node view, from the View menu, choose **Go to Network View**. Otherwise, go to Step 2.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**. A BLSR window is displayed containing a graphic of the BLSR.

Step 4 On the BLSR network graphic click an icon and while pressing **Ctrl**, drag the icon to a new location so you can see the BLSR port information clearly.

Step 5 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 5-7 on page 5-23 shows an example. (To move a graphic icon, click it, press **Ctrl**, and drag the icon to a new location.)

Note For four-fiber BLSRs, the squares represent ports. Right-click either working port.

b. On the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down menu. Click **OK**.

c. Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed on the working BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the force was invoked, and all span lines between other BLSR nodes turn green.

Step 6 Click the **Conditions** tab, then click **Retrieve**.

Step 7 Verify that a SPAN-SW-WEST (Span Switch West) condition is reported on the node where you invoked the force 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 (not depressed). Click the Node column to sort conditions by node.

Step 8 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 9 Display the BLSR window where you invoked the force span switch (the window may be hidden by the CTC window).

Step 10 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. On the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

c. Click **Yes** on the Confirm BLSR Operation dialog box.

On the network graphic, the F indicating the force span 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 11 Switch the east span:

a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.

b. On the Set East Protection Operation dialog box, choose **FORCE SPAN** from the drop-down menu. Click **OK**.

c. Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed on the working BLSR channel where you invoked the force ring switch. The BLSR span lines are purple where the force was invoked, and all span lines between other BLSR nodes are green. The span lines may take a few moments to change color.

Step 12 Click the **Conditions** tab, then click **Retrieve**.

Step 13 Verify that a SPAN-SW-EAST (Span Switch East) condition is reported on the node where you invoked the force 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 (not depressed). Click the Node column to sort conditions by node.

Step 14 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide.*

Step 15 Display the BLSR window where you invoked the force span switch (the window may be hidden by the CTC window).

Step 16 Clear the east switch:

a. Right-click the east port of the BLSR node where you invoked the force ring switch and choose **Set East Protection Operation**.

b. On the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

c. Click **Yes** on the Confirm BLSR Operation dialog box.

On the network graphic, the F indicating the force ring 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 17 Close the BLSR window: from the File menu, choose **Close**.

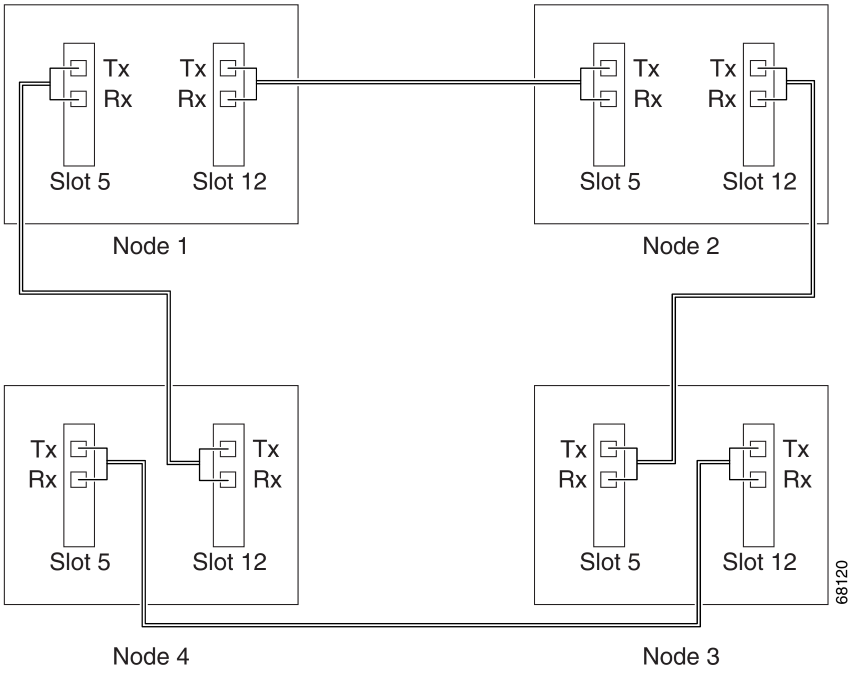
Step 18 Return to your originating procedure (NTP).

NTP-44 Provision UPSR Nodes

Purpose	Use this procedure to provision nodes for inclusion in a unidirectional path switched ring.
Tools/Equipment	None
Prerequisite Procedures	NTP-35 Verify Node Turn Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the UPSR trunk OC-N cards similar to Figure 5-8.

Figure 5-8 UPSR fiber connection example



Step 2 Log into an ONS 15454 in the UPSR you are turning up. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 3 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for the two cards/ports that will serve as the UPSR 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 provisioning must be performed through a local craft connection. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 4 Repeat Steps 2–3 for each node in the UPSR.

Step 5 Complete the "NTP-45 UPSR Acceptance Test" procedure on page 5-33.

NTP-45 UPSR Acceptance Test

Purpose	Use this procedure to test an ONS 15454 UPSR.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-44 Provision UPSR Nodes, page 5-31
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into one of the ONS 15454s on the UPSR you are testing. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Alarms** tab. Verify that no unexplained alarms are displayed on the network. If unexplained alarms are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Export the alarms data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 5 Click the **Conditions** tab. Verify that no unexplained conditions are displayed on the network. If unexplained conditions are displayed, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Export the conditions data to a file by choosing **Export** from the File menu. Select an export format and save the file to your hard drive. See the "DLP-139 Export CTC Data" task on page 7-3 for additional information.

Step 7 On the network map, double-click the node that you logged into in Step 1.

Step 8 Create a test circuit from that node to the next adjacent UPSR node.

- For DS-1 circuits, complete the "NTP-128 Create an Automatically Routed DS-1 Circuit" procedure on page 6-6. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.
- For DS-3 circuits, complete the "NTP-131 Create an Automatically Routed DS-3 Circuit" procedure on page 6-17. When you set the circuit state, choose **IS** and check the **Apply to drop ports** checkbox.

Step 9 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. After you choose muxed DS-3, choose the DS-1 to test on the muxed DS-3. 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) the other to the test set receive (Rx). 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)

b. Attach the other end to the port's receive (Rx).

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 displays a clean signal. If a clean signal is not displayed, repeat Steps 1–10 to make sure the test set and cabling is 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 display at the test set.

Step 15 Complete the "DLP-215 TCC+ Active/Standby Switch Test" task on page 5-8.

Step 16 Complete the "DLP-216 Cross-Connect Card Active/Standby Switch Test" task on page 5-10.

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 Test the UPSR protection switching function on this span. Go to the "DLP-94 UPSR Protection Switching Test" task on page 5-35 for instructions.

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 20 In network view, click the other circuit source span.

Step 21 Test the UPSR protection switching function on this span. Go to the "DLP-94 UPSR Protection Switching Test" task on page 5-35 for instructions.

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 22 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 23 Complete the "NTP-152 Delete Circuits" procedure on page 9-11 for the test circuit.

Step 24 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete.

Step 25 View the alarms and conditions on each node and record results by exporting to a file. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 26 Repeat Steps 8–22 for each node on the network.

Step 27 If a node fails any test, repeat the test 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 6, "Create Circuits and VT Tunnels."

DLP-94 UPSR Protection Switching Test

Purpose	Use this task to verify that a UPSR span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 displays the UPSR circuits, including circuit names, location, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span** switching field and choose **FORCE SWITCH AWAY** from the pull-down menu. Click **Apply**.

Step 4 On the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 On the Protection Switch Result dialog box, click **OK**.

On the Circuits on Span dialog box, the Switch State for all circuits is FORCE. Unprotected circuits will not switch.

Step 6 Click the **Perform UPSR span switching** field and choose **CLEAR** from the pull-down menu. Click **Apply**. Click **Yes** to confirm.

Step 7 On the Confirm UPSR Switch dialog box, click **Yes**.

Step 8 On the Protection Switch Result dialog box, click **OK**.

On the Circuits on Span window, the Switch State for all UPSR circuits is CLEAR.

NTP-46 Subtend a UPSR from a BLSR

Purpose	Use this procedure to subtend a UPSR from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers to carry the UPSR.
Prerequisite Procedures	NTP-42 Two-Fiber BLSR Acceptance Test, page 5-21 or NTP-43 Four-Fiber BLSR Acceptance Test, page 5-26
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the node that will subtend the UPSR (Node 3 in Figure 5-9), install the OC-N cards that will serve as the UPSR trunk cards (Node 3, Slots 6 and 13). If they are already installed, go to Step 2.

Step 2 Attach fibers from these cards to the UPSR trunk cards on the UPSR nodes. In Figure 5-9, Slot 6/Node 3 connects to Slot 13/Node 5, and Slot 13/Node 5 connects to Slot 6/Node 6.

Step 3 Log into the ONS 15454 that will subtend the UPSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 4 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for each OC-N card that will carry the UPSR.

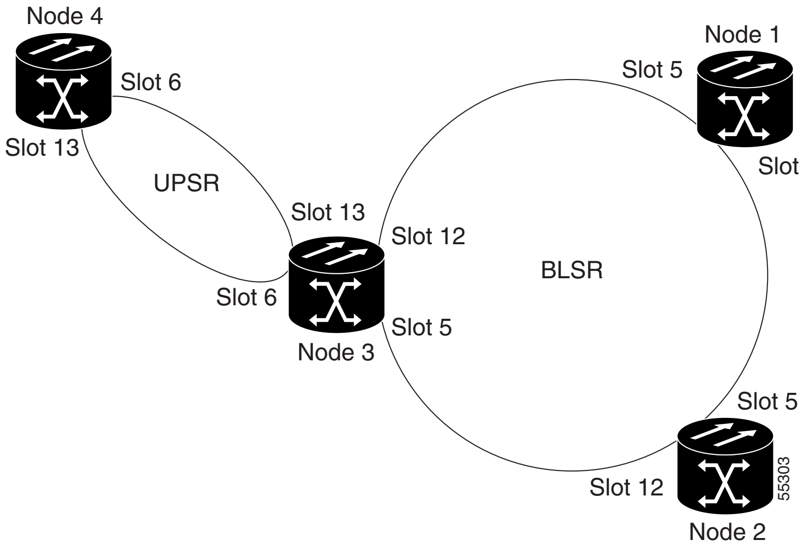
Step 5 Log into the UPSR node that connects to the node in Step 3.

Step 6 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for each OC-N card that will carry the UPSR.

Step 7 Repeat Step 6 for each node in the UPSR.

Step 8 From the View menu, choose **Go To Network View**.

Figure 5-9 A UPSR subtending from a BLSR



Step 9 Complete the "NTP-45 UPSR Acceptance Test" procedure on page 5-33.

NTP-47 Subtend a BLSR from a UPSR

Purpose	Use this procedure to subtend a BLSR from an existing UPSR.
Tools/Equipment	One UPSR node must have OC-N cards and fibers to carry the BLSR.
Prerequisite Procedures	NTP-45 UPSR Acceptance Test, page 5-33
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the node that will subtend the BLSR, install the OC-N cards that will serve as the BLSR trunk cards (in Figure 5-9, Node 3, Slots 6 and 13).

Step 2 Attach fibers from the cards in Step 1 to the BLSR trunk cards on another BLSR node. In Figure 5-9, Slot 6/Node 3 connects to Slot 13/Node 5, and Slot 13/Node 5 connects to Slot 6/Node 6.

Step 3 Log into the ONS 15454 that will subtend the BLSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The node (default) view displays.

Step 4 Create the DCCs on both OC-N cards (east and west) that will carry the BLSR. See the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for instructions.

Step 5 Create the subtending BLSR:

a. Complete the "NTP-40 Provision BLSR Nodes" procedure on page 5-16 for each node that will be in the BLSR.

b. Complete the "NTP-126 Create a BLSR" procedure on page 5-19. Include the node in Step 3 (the node that will subtend the BLSR) in the BLSR.

Step 6 Go to the network view to see the subtending ring.

NTP-48 Subtend a BLSR from a BLSR

Purpose	Use this procedure to subtend a BLSR from existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers to carry the second BLSR.
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

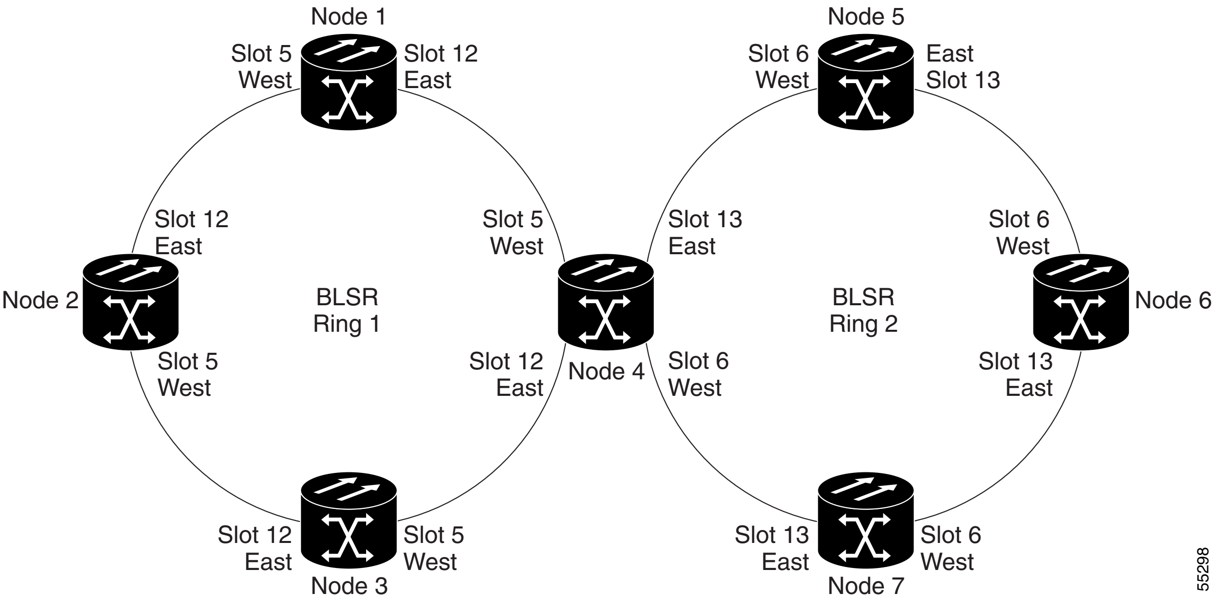
Note This procedure assumes that all nodes are configured for the BLSR. If you need to add a node to a BLSR, see the "NTP-160 Add a BLSR Node" procedure on page 14-2.

Step 1 Log into the node that will subtend the BLSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Install the OC-N cards that will serve as the BLSR trunk cards if they are not already installed. See the "NTP-16 Install the Optical Cards" procedure on page 2-11.

Figure 5-10 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 5-10 A BLSR subtending from a BLSR



Step 3 Attach fibers from these cards to the BLSR trunk cards on the BLSR nodes. In Figure 5-10, 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-213 Provision SONET DCC Terminations" task on page 5-4 for instructions.

Step 5 Repeat Step 4 for the second OC-N trunk card that will carry the BLSR.

Step 6 Complete the "NTP-126 Create a BLSR" procedure on page 5-19 to provision the new BLSR. The subtending BLSR must have a ring ID that differs from the ring ID of the first BLSR. 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.

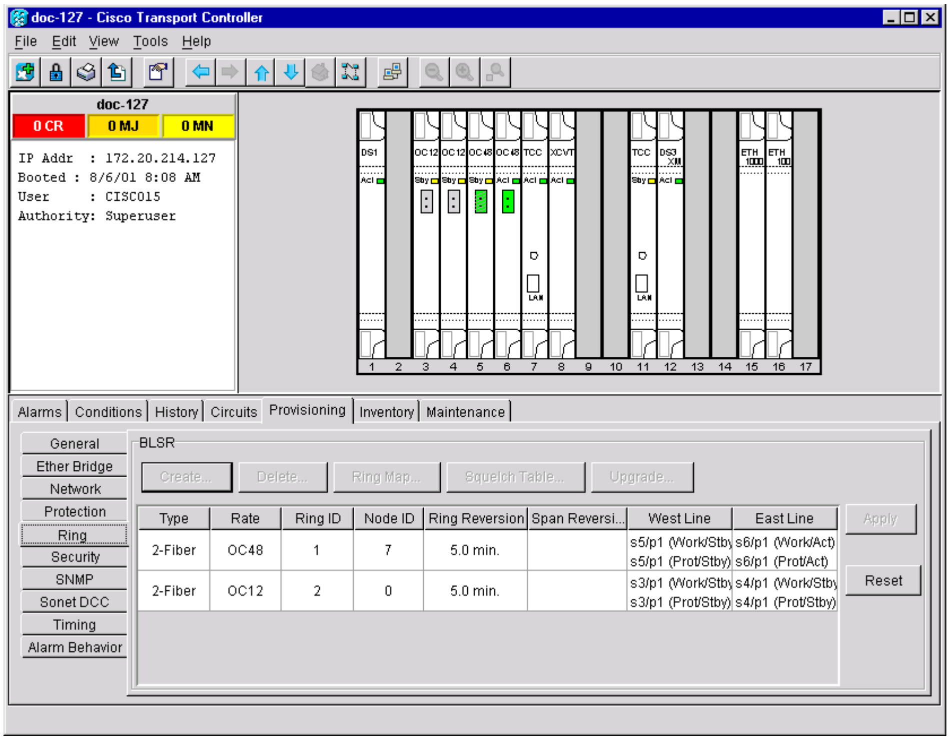
Step 7 Display the network view to see the subtending ring.

Figure 5-11 shows an example of two subtending BLSRs.

Figure 5-11 Viewing subtending BLSRs on the network map

Figure 5-12 shows the Ring subtab for Node 5, which is the node that carries the two rings.

Figure 5-12 Configuring two BLSRs on the same node



IP Addr : 172.20.214.127
Booted : 8/6/01 8:08 AM
User : CISCO15
Authority: Superuser

Type	Rate	Ring ID	Node ID	Ring Reversion	Span Reversi...	West Line	East Line
2-Fiber	OC48	1	7	5.0 min.		s5/p1 (Work/Stby s5/p1 (Prot/Stby)	s6/p1 (Work/Act) s6/p1 (Prot/Act)
2-Fiber	OC12	2	0	5.0 min.		s3/p1 (Work/Stby s3/p1 (Prot/Stby)	s4/p1 (Work/Stby s4/p1 (Prot/Stby)

Step 8 Complete the "NTP-42 Two-Fiber BLSR Acceptance Test" procedure on page 5-21 or the "NTP-43 Four-Fiber BLSR Acceptance Test" procedure on page 5-26 depending on the type of BLSR.

NTP-49 Create a DCC Tunnel

Purpose	Use this procedure to create a 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-35 Verify Node Turn Up, page 5-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15454 can have up to 32 DCC tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as a DCC tunnel end-point, and a Section DCC that is used as an DCC tunnel end-point cannot be terminated. All DCC tunnel connections are bidirectional.

Step 1 Log into an ONS 15454 that is connected to the non-ONS 15454 network.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning > Overhead Circuits** tabs.

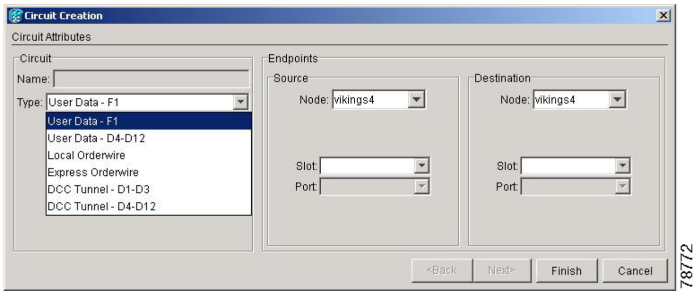
Step 4 Click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-13), provision the DCC tunnel:

- Name—Type the tunnel name.
- 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.
- Source Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, select the source port.
- Channel—Is displayed if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—is the Section DCC
  - DCC2 (D4-D6)—is Line DCC 1
  - DCC3 (D7-D9)—is Line DCC 2
  - DCC4 (D10-D12)—is Line DCC 3

  DCC options are not displayed if they are used by the ONS 15454 (DCC1) or other tunnels.

Figure 5-13 Provisioning a DCC tunnel



Circuit Creation

Circuit Attributes

Circuit

Name:

Type: User Data - F1

Endpoints

Source

Node: vikings4

Slot:

Port:

Destination

Node: vikings4

Slot:

Port:

Step 6 Click **OK**.

Step 7 Put the ports hosting the DCC tunnel in service. See the "DLP-214 Change the Service State for a Port" task on page 5-5 for instructions.

CHAPTER 6

Create Circuits and VT Tunnels

This chapter explains how to create Cisco ONS 15454 electrical circuits, VT tunnels, optical circuits, and Ethernet circuits. For additional information about ONS 15454 circuits, refer to the Circuits and Tunnels chapter in the *Cisco ONS 15454 Reference Guide*.

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-127 Verify Network Turn Up, page 6-4—Complete this procedure before you create any circuits.
2. NTP-128 Create an Automatically Routed DS-1 Circuit, page 6-6—Complete as needed.
3. NTP-129 Create a Manually Routed DS-1 Circuit, page 6-10—Complete as needed.
4. NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12—Complete as needed.
5. NTP-131 Create an Automatically Routed DS-3 Circuit, page 6-17—Complete as needed.
6. NTP-132 Create a Manually Routed DS-3 Circuit, page 6-21—Complete as needed.
7. NTP-56 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 6-23—Complete as needed.
8. NTP-133 Create an Automatically Routed VT Tunnel, page 6-30—Complete as needed.
9. NTP-134 Create a Manually Routed VT Tunnel, page 6-33—Complete as needed.
10. NTP-135 Test Electrical Circuits, page 6-36—Complete this procedure after you create an electrical circuit.
11. NTP-136 Create an Automatically Routed Optical Circuit, page 6-38—Complete as needed.
12. NTP-137 Create a Manually Routed Optical Circuit, page 6-41—Complete as needed.
13. NTP-138 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-44—Complete as needed.
14. NTP-62 Test Optical Circuits, page 6-50—Complete this procedure after you create an optical circuit.
15. NTP-139 Create a Half Circuit on a BLSR or 1+1 Node, page 6-52—Complete this procedure as needed to create a half circuit using an OC-N as a destination in BLSR or 1+1.

16. NTP-140 Create a Half Circuit on a UPSR Node, page 6-54—Complete this procedure as needed to create a half circuit using an OC-N as a destination in UPSR.
17. NTP-141 Provision an E Series EtherSwitch Circuit (Multicard or Single-Card), page 6-56—Complete this procedure as needed to create E Series EtherSwitch circuits.
18. NTP-142 Create an E Series Shared Packet Ring Ethernet Circuit, page 6-59—Complete this procedure as needed to create E Series shared packet ring Ethernet circuits.
19. NTP-143 Create an E Series Hub and Spoke Ethernet Configuration, page 6-63—Complete this procedure as needed to create E Series hub and spoke circuits.
20. NTP-144 Provision an E Series Single-Card EtherSwitch Manual Cross-Connect, page 6-66—Complete this procedure as needed to create single-card EtherSwitch manual cross connects.
21. NTP-145 Provision an E Series Multicard EtherSwitch Manual Cross-Connect, page 6-68—Complete this procedure as needed to create multicard EtherSwitch manual cross connects.
22. NTP-146 Test E Series Ethernet Circuits, page 6-77—Complete this procedure after creating E series Ethernet circuits.
23. NTP-147 Create a G1000-4 Ethernet Circuit, page 6-78—Complete this procedure as needed to create a G1000-4 EtherSwitch circuit.
24. NTP-148 Provision a G1000-4 Manual Cross-Connect, page 6-80—Complete this procedure as needed to create multicard G1000-4 manual cross connects.
25. NTP-149 Test G Series Ethernet Circuits, page 6-83—Complete this procedure after creating G series Ethernet circuits.

Table 6-1 defines ONS 15454 circuit creation terms and options.

Table 6-1 ONS 15454 Circuit Options

Circuit Option	Description
Source	The point where the circuit enters the ONS 15454 network.
Destination	The point where the circuit exits an ONS 15454 network.
Automatic circuit routing	CTC routes the circuit automatically on the shortest available path based on the routing parameters that you define and on bandwidth availability.
Manual circuit routing	Allows you to choose a specific path, not just the shortest path chosen by automatic routing. You can choose a specific STS or VT for each circuit segment and create circuits from work orders prepared by an operations support system (OSS) like the Telcordia TIRKS system
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 will use cross-connect capacity only at the source and destination nodes. One VT tunnel can carry 28 VT1.5 circuits.

ONS 15454 circuits are either a VT or an STS circuit. Table 6-2 shows the circuit source and destination options that display for VT circuits. Table 6-3 shows the options that display for STS circuits.

Table 6-2 Source and Destination Options For VT Circuits

Card	Ports	STSs	VTs	DS1s
DS1-14, DS1N-14	–	–	–	14
DS3-12, DS3N-12, DS3-12E, DS3N-12E	–	–	–	–
DS3XM-6	6	–	–	28 per port
EC1-12	12	–	28 per port	–
OC3 IR 4/STM1	4	3 per port	28 per STS	–
OC12 IR/STM4 OC12 LR/STM4	–	12	28 per STS	–
OC12 IR 4/STM4 OC12 LR 4/STM4	4	12 per port	28 per STS	–
All OC48 cards	–	48	28 per STS	–
OC192	–	192	28 per STS	–

Table 6-3 Source and Destination Options that Display for STS Circuits

Card	Ports	STSs	Notes
DS1-14, DS1N-14	–	–	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.
DS3-12, DS3N-12, DS3-12E, DS3N-12E	12	–	
DS3XM-6	6	–	
EC1-12	12	–	
OC3 IR 4/STM1	4	3 per port	
OC12 IR/STM4 OC12 LR/STM4	–	12	
OC12 IR 4/STM4 OC12 LR 4/STM4	4	12 per port	
All OC48 cards	–	48	
OC192	–	192	

NTP-127 Verify Network Turn Up

Purpose	This procedure verifies that the ONS 15454 network is ready for circuit provisioning.
Tools/Equipment	None
Prerequisite Procedures	Chapter 5, "Turn Up Network"
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15454 on the network where you will create circuits. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 From the View menu, choose **Go to Network View**. Wait for all the nodes that are part of the network to display on the network map. (Large networks may 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 will be stacked on the left side of your screen, possibly out of view. Use the scroll bar beneath the network map to display the icons. To separate the icons press **Ctrl** and click and drag the icon with your mouse to the new location. Repeat until all the nodes are visible on the screen.

Step 3 Verify node accessibility. All node icons must be either green, yellow, orange, or red.

If all network nodes do not display after a few minutes, or if a node icon is grey with an IP address under it, do not continue. Check the Net box in the lower right corner of the window. If it is grey, log in again, making sure not to check the Disable Network checkbox on the CTC Login dialog box. If problems persist, see Chapter 5, "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 grey in color, do not continue. See Chapter 5, "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 Investigate and resolve, if necessary, all critical (red node icon) or major (orange node icon) alarms. Click the **Alarms** tab to view alarm descriptions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* to resolve the alarm 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 displayed 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 NTP/SNTP server IP address (if used) are correctly provisioned. If needed, make corrections using the "NTP-25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-3.

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-26 Set Up CTC Network Access" procedure on page 4-5.

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-29 Create Protection Groups" procedure on page 4-23.

e. If the node is in a BLSR, click the **BLSR** tab. (If the node is not in a BLSR, proceed to 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 corrections need to be made, see the "NTP-40 Provision BLSR Nodes" task on page 5-16 for instructions.

f. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-30 Create Users and Assign Security" procedure on page 4-28 to correct the information.

g. If SNMP is used, click the **SNMP** tab and verify the trap and destination information. If the information is not correct, see the "NTP-33 Set Up SNMP" procedure on page 4-38 to correct the information.

h. Click the **Sonet DCC** tab. Verify that DCC(s) were created to the applicable OC-N cards and ports. If DCCs were not created for the appropriate OC-N cards, see Chapter 5, "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-28 Set Up Timing" procedure on page 4-18 to make the changes.

j. Click the **Alarm Behavior** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 7-16 to change the information.

k. Verify that the network elements defaults listed in the status area of the node view window is correct.

Step 7 Choose the next node in the network and repeat Step 6 for that node. Repeat for each node in the network.

Step 8 As appropriate, complete the circuit creation procedure listed on page 6-1.

NTP-128 Create an Automatically Routed DS-1 Circuit

Purpose	This procedure creates an automatically routed DS-1 circuit, meaning CTC chooses the circuit route based on the parameters you set at circuit creation and on the system load.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose VT. VT cross connects will carry the DS-1 circuit across the ONS 15454 network.
- *Size*—VT1.5 is the default. You cannot change it.
- *Bidirectional*—Leave checked for this circuit (default).
- *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, consecutive port numbers, you can use Auto-ranged to create the circuits automatically.
- *Auto-ranged*—This checkbox 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. Deselect the box if you do not want CTC to create sequential circuits automatically.
- *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—(default) 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-230 Change a Circuit State" task on page 9-7.

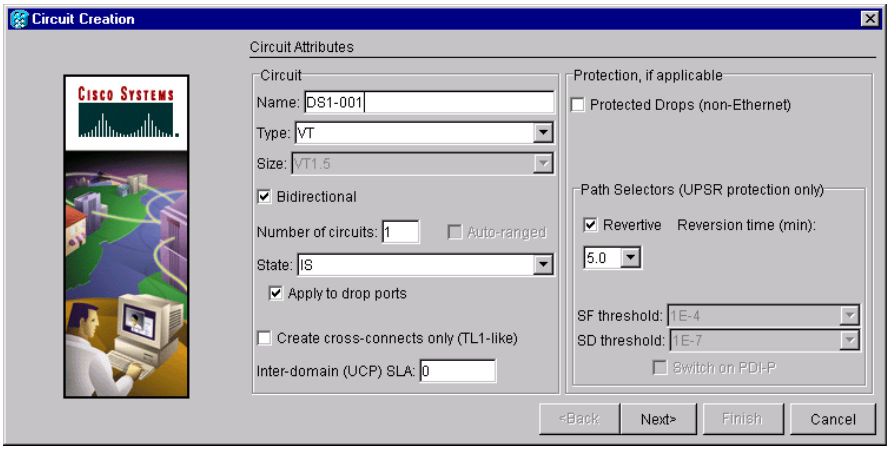
Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Guide* for more information.

- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS 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, and VT tunnels, Ethergroup sources, and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Click 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 choose this box, CTC only displays protected cards and ports as source and destination choices.

Figure 6-1 Setting circuit attributes for a DS-1 circuit



Circuit Attributes

Circuit
Name: DS1-001
Type: VT
Size: VT1.5
☑ Bidirectional
Number of circuits: 1 □ Auto-ranged
State: IS
☑ Apply to drop ports
□ Create cross-connects only (TL1-like)
Inter-domain (UCP) SLA: 0

Protection, if applicable
□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)
☑ Revertive Reversion time (min): 5.0
SF threshold: 1E-4
SD threshold: 1E-7
□ Switch on PDI-P

Step 5 Click **Next**.

Step 6 Complete the "DLP-95 Provision a DS-1 Circuit Source and Destination" task on page 6-15.

Step 7 Beneath Circuit Routing Preferences (Figure 6-2 on page 6-8), choose **Route Automatically**. The following options are available.

- *Using Required Nodes/Spans*—Click this box if you want to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- *Review Route Before Creation*—Click this box if you want to review and edit the circuit route before the circuit is created.

Choose either, both, or none, based on your preferences.

Step 8 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 9. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.

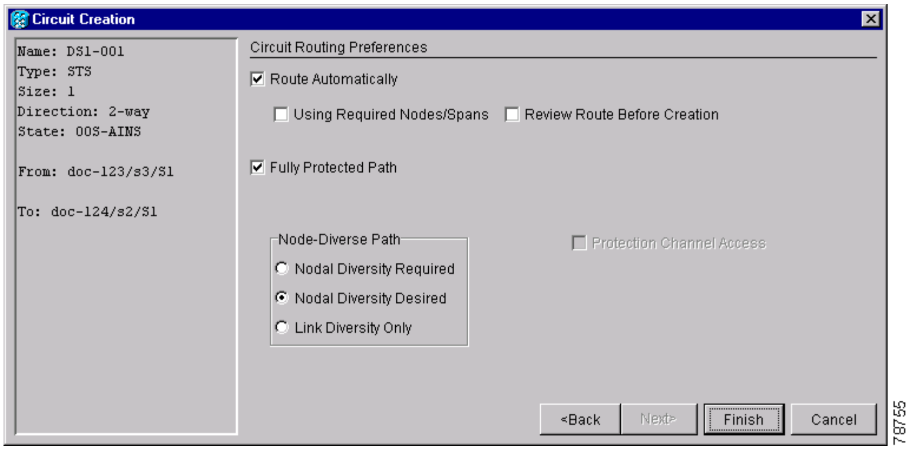
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 10.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 10.

Caution Circuits routed on PCA are not protected and are pre-empted during BLSR ring and span switches.

Step 9 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 6-2 Setting circuit routing preferences for a DS-1 circuit



Circuit Creation

```
Name: DS1-001
Type: STS
Size: 1
Direction: 2-way
State: OOS-AINS

From: doc-123/s3/S1

To: doc-124/s2/S1
```

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path

○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access

Step 10 If you selected Using Required Nodes/Spans, complete the following substeps. If not, proceed to Step 11.

a. Click **Next**.

If the VT circuit is routed through a node and a VT tunnel is not present, a VT Tunnel Creation dialog box is displayed asking whether you want to create a VT tunnel on the transit node. If many VT circuits (over 14) will pass through the same node, click **Yes**. If you are only creating a few VT circuits, pick **No**.

b. Beneath Circuit Route Constraints, 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/span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be 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 under 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 11 If you selected Review Route Before Creation, complete the following substeps. If not, proceed to Step 12.

a. Click **Next**.

b. If the DS-1 circuit passes through a node that does not have a VT tunnel, CTC will ask whether you want to create one. See Step 12 for information about the VT tunnel.

c. 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.

d. 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-129 Create a Manually Routed DS-1 Circuit" task on page 6-10.

Step 12 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing tunnel is full, CTC asks whether you want to create tunnel. 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 Guide* for more information.
- If you entered more than 1 in *Number of circuits* 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 is displayed. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in *Number of circuits* and did not choose *Auto-ranged*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 13 On the Circuits window, verify that the circuit(s) just created appear in the circuits list.

Step 14 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-129 Create a Manually Routed DS-1 Circuit

Purpose	This procedure creates a DS-1 circuit and allows you to route the circuit path manually.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (see Figure 6-1 on page 6-7), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose VT. VT cross connects will carry the DS-1 circuit across the ONS 15454 network.
- *Size*—VT1.5 is the default. You cannot change it.
- *Bidirectional*—Leave checked for this circuit (default).
- *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 *Number of Circuits*, deselect this box. (The box is unavailable if only one circuit is entered in *Number of Circuits*.)
- *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—(default) 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-230 Change a Circuit State" task on page 9-7.

Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Guide* 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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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, and VT tunnels, Ethergroup sources, and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (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 choose this box, CTC only displays protected cards and ports as source and destination choices.

Step 5 Click **Next**.

Step 6 Complete the "DLP-95 Provision a DS-1 Circuit Source and Destination" task on page 6-15.

Step 7 Beneath Circuit Routing Preferences (see Figure 6-2 on page 6-8), deselect **Route Automatically**.

Step 8 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 9. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 10.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 10.

Caution Circuits routed on PCA are not protected and are pre-empted during BLSR ring and span switches.

Step 9 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*— (default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 10 Click **Next**. Beneath Route Review and Edit, node icons are displayed 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 11 Complete the "DLP-96 Provision a DS-1 or DS-3 Circuit Route" task on page 6-28 for the DS-1 circuit you are creating.

Step 12 Click **Finish**. CTC will compare your manually-provisioned circuit route with the specified path diversity option. 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 *Number of circuits*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.

Step 13 When all the circuits are created, CTC displays the main Circuits window. Verify that the circuit(s) you created are correct.

Step 14 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-1 circuit with multiple drops.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose VT.
- *Size*—VT1.5 is the default. You cannot change it.
- *Bidirectional*—Deselect for this circuit.
- *Number of circuits*—Leave the default unchanged (1).
- *Auto-ranged*—Unavailable when *Number of Circuits* is 1.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.

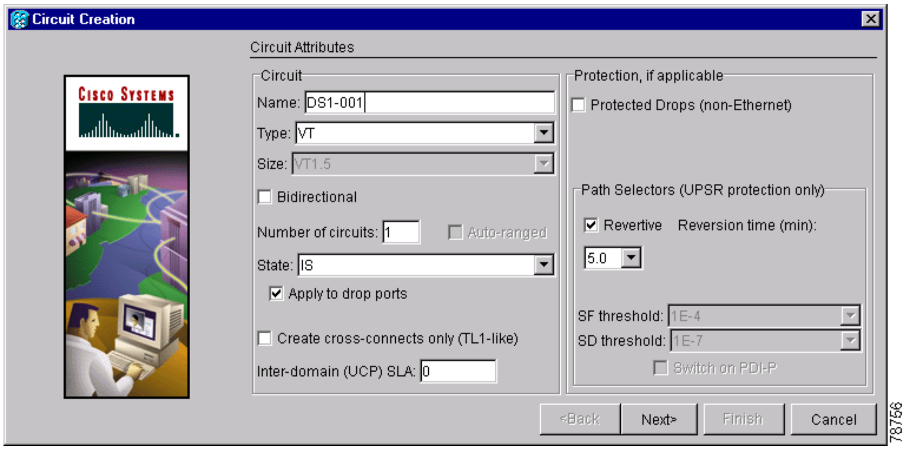
Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15454 Reference Guide* for more information.

- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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, and VT tunnels, Ethergroup sources, and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (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 only displays protected cards as source and destination choices.

Figure 6-3 Setting circuit attributes for a unidirectional DS-1 circuit


Circuit Creation

Circuit Attributes

Circuit

Name: DS1-001

Type: VT

Size: VT1.5

□ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 Click **Next**.

Step 6 Complete the "DLP-95 Provision a DS-1 Circuit Source and Destination" task on page 6-15.

Step 7 Beneath Circuit Routing Preferences, deselect **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 8 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 9. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 10.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 10.

Caution Circuits routed on PCA are not protected. They are pre-empted during BLSR ring and span switches.

Step 9 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 10 Click **Next**. Beneath Route Review and Edit, node icons are displayed 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 11 Complete the "DLP-96 Provision a DS-1 or DS-3 Circuit Route" task on page 6-28 for the DS-1 circuit you are creating.

Step 12 Click **Finish**. CTC completes the circuit and displays the Circuits window.

Step 13 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 14 Click **Edit**. The Edit Circuit window is displayed with the General tab selected.

All nodes in the DCC network are displayed on the network. Circuit source and destination information appears under the source and destination nodes. To display a detailed view of the circuit, click **Show Detailed Map**. You can also rearrange a node icon by selecting the node with the left mouse button while simultaneously pressing **Ctrl**, then dragging the icon to the new location.

Step 15 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops is displayed.

Step 16 Click **Create**.

Step 17 On 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 pull-down menus. The card selected in Step b determines the fields that display. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

   – If the original circuit was routed on a protected path, you can change the nodal diversity options: [Required, Desired, Don't Care; Link Diverse only]. See Step Step 9 for options descriptions.

   – If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 8 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 18 If you need to create additional drops for the circuit, repeat Step 16–17 to create the additional drops.

Step 19 Choose **Close**. The Circuits window is displayed.

Step 20 Verify that the new drops are displayed under the Destination column for the circuit you edited. If they do not appear repeat Steps 4–20, making sure all options are provisioned correctly.

Step 21 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

DLP-95 Provision a DS-1 Circuit Source and Destination

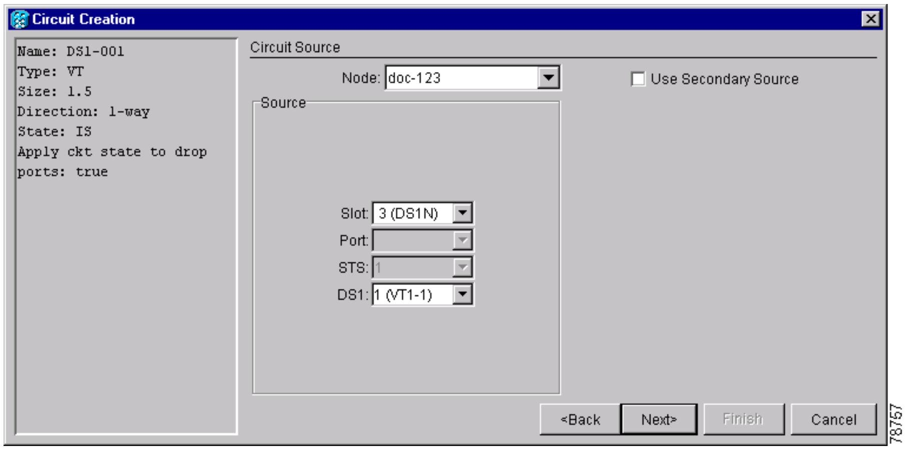
Purpose	This task provisions an electrical circuit source and destination for a DS-1 circuit.
Tools/Equipment	None
Prerequisite Procedures	You perform this task during one of the following procedures: NTP-128 Create an Automatically Routed DS-1 Circuit, page 6-6, or NTP-129 Create a Manually Routed DS-1 Circuit, page 6-10, or NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12
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 pull-down menu, choose the node where the source will originate.

Step 2 From the Slot pull-down menu, choose the slot containing the DS1-14, DS1N-14 (Figure 6-4), or DS3XM-6 (Figure 6-5) card where the circuit will originate.

Figure 6-4 Defining the circuit source on a DS1N-14 card



```
Name: DS1-001
Type: VT
Size: 1.5
Direction: 1-way
State: IS
Apply ckt state to drop
ports: true
```

Node: doc-123

□ Use Secondary Source

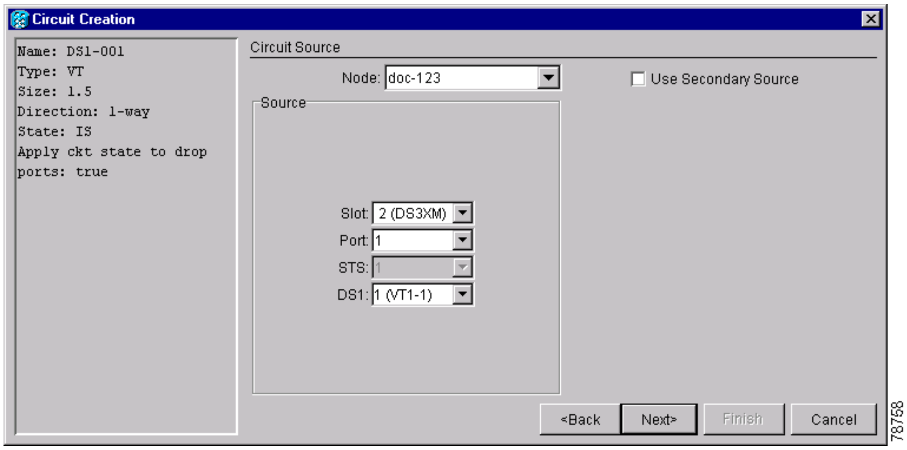
Slot: 3 (DS1N)

Port:

STS: 1

DS1: 1 (VT1-1)

Figure 6-5 Defining the circuit source on a DS3XM-6 card



```
Name: DS1-001
Type: VT
Size: 1.5
Direction: 1-way
State: IS
Apply ckt state to drop
ports: true
```

Node: doc-123

□ Use Secondary Source

Slot: 2 (DS3XM)

Port: 1

STS: 1

DS1: 1 (VT1-1)

Step 3 Only if you chose DS3XM-6 as the card, choose the port from the Port pull-down menu.

Step 4 From the DS-1 pull-down menu, choose the source DS-1.

Step 5 If you need to create a secondary source, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1–4 to define the secondary source. If you do not need to create a secondary source, proceed to Step 6.

Step 6 Click **Next**.

Step 7 From the Node pull-down menu, choose the destination (termination) node.

Step 8 From the Slot pull-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 optical transport.

Step 9 Depending on the destination card, choose the destination port, STS, VT, or DS1 from the sub-menus that display based on the card selected in Step 8. See Table 6-2 on page 6-3 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s already used 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 will receive a Path in Use error and be 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 UPSR bridge/selector circuit exit point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 7–9 to define the secondary destination.

Step 11 Click **Next**.

Step 12 Finish the circuit creation procedure that referred you to this task.

NTP-131 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 system load.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1), complete the following fields:

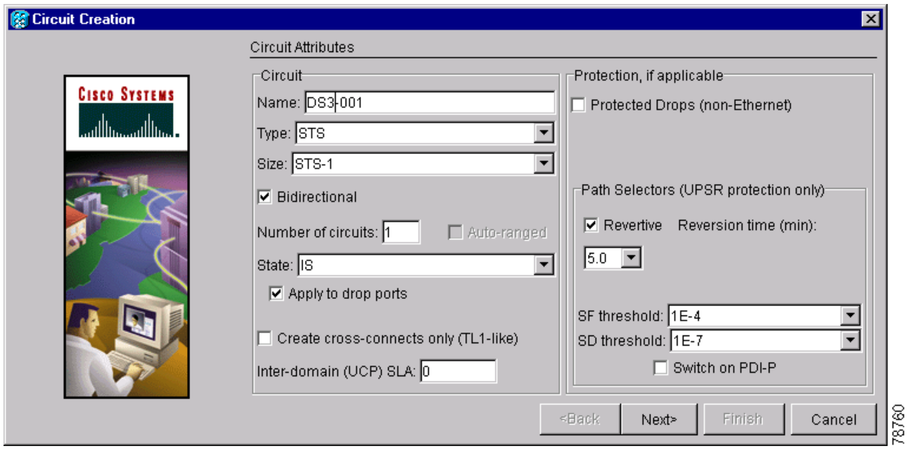
- *Name*—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- *Type*—Choose STS. STS cross connects will carry the DS-3 circuit across the ONS 15454 network.
- *Size*—Choose STS-1.
- *Bidirectional*—Leave checked for this circuit (default).
- *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. Deselect the box if you do not want CTC to create sequential circuits automatically.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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, and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (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 only displays protected cards and ports as source and destination choices.

Figure 6-6 Setting circuit attributes for a DS-3 circuit



Circuit Creation

Circuit Attributes

Circuit

Name: DS3-001

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 If the circuit will be routed on a UPSR, complete the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Complete the "DLP-208 Provision a DS-3 Circuit Source and Destination" task on page 6-27.

Step 8 Beneath Circuit Routing Preferences (Figure 6-7 on page 6-19), choose **Route Automatically**. The following options are available:

- *Using Required Nodes/Spans*—Choose this box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- *Review Route Before Creation*—Choose this box to review and edit the circuit route before the circuit is created.

Step 9 Set the circuit path protection:

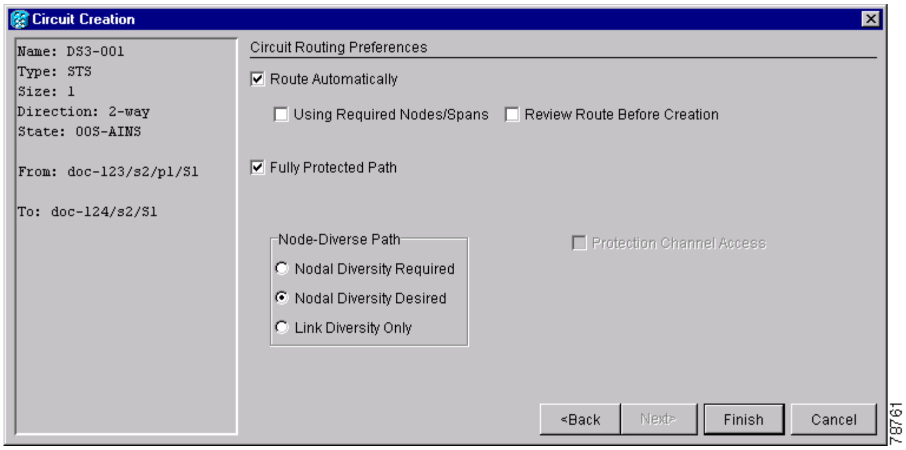
- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 10. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 11.

Caution Circuits routed on PCA are not protected and are pre-empted during BLSR ring and span switches.

Step 10 If you selected Fully Protected Path choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 6-7 Setting circuit routing preferences for a DS-3 circuit



Circuit Creation

Name: DS3-001
Type: STS
Size: 1
Direction: 2-way
State: OOS-AINS

From: doc-123/s2/p1/S1

To: doc-124/s2/S1

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access

Step 11 If you selected Using Required Nodes/Spans complete the following substeps; otherwise, proceed to Step 12:

a. Click **Next**.

b. Beneath Circuit Route Constraints, 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/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 grey, that node or span is required.

Step 12 If you selected Review Route Before Creation, complete the following substeps; otherwise, proceed to Step 13.

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-132 Create a Manually Routed DS-3 Circuit" procedure on page 6-21.

Step 13 Click **Finish**. One of the following actions occurs based on the circuit properties you selected:

- If you entered more than 1 in *Number of circuits* 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 is displayed. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in *Number of circuits* and did not choose *Auto-ranged*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat Steps 7–13 for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 14 On the Circuits window, verify that the circuit(s) you just created appear in the circuits list.

Step 15 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-132 Create a Manually Routed DS-3 Circuit

Purpose	This procedure creates a DS-3 circuit and allows you to choose the circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the node where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1 on page 6-7), complete the following fields:

- *Name*—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave this field blank, CTC will assign a default name to the circuit.
- *Type*—Choose STS. STS cross-connects will carry the DS-3 circuit across the ONS 15454 network.
- *Size*—Choose STS-1.
- *Bidirectional*—Leave this field checked (default).
- *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 *Number of Circuits*, deselect this box. (The box is unavailable if only one circuit is entered in *Number of Circuits*.)
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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, and VT tunnels, Ethergroup sources, and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Choose 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 choose this box, CTC only displays protected cards as source and destination choices.

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Complete the "DLP-208 Provision a DS-3 Circuit Source and Destination" task on page 6-27.

Step 8 Beneath Circuit Routing Preferences (Figure 6-7 on page 6-19), deselect **Route Automatically**.

Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 9. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 11.

⚠ **Caution** Circuits routed on PCA are not protected and are pre-empted during BLSR ring and span switches.

Step 10 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 11 Click **Next**. Beneath Route Review and Edit, node icons are displayed 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 12 Complete the "DLP-96 Provision a DS-1 or DS-3 Circuit Route" task on page 6-28 for the DS-3 you are creating.

Step 13 Click **Finish**. If you entered more than 1 in *Number of circuits*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.

Step 14 When all the circuits are created, CTC displays the main Circuits window. Verify that the circuit(s) you created appear in the window.

Step 15 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-56 Create a Unidirectional DS-3 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-3 circuit with multiple drops.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1 on page 6-7), complete the following fields:

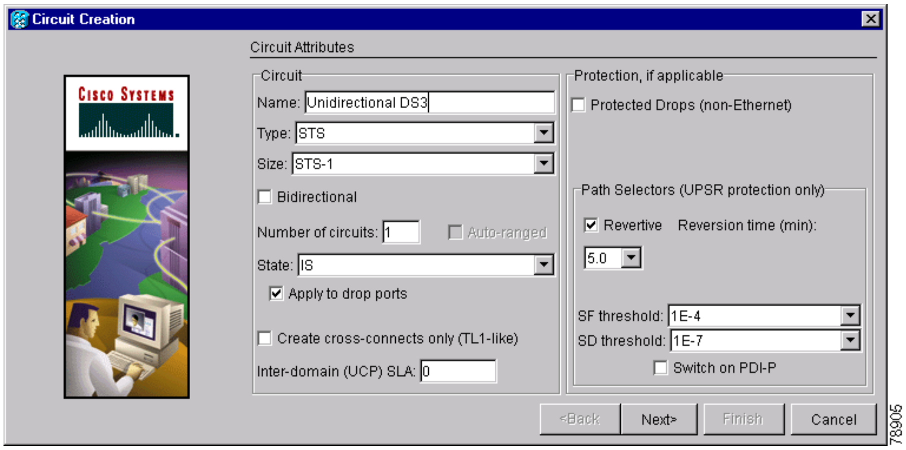
- *Name*—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- *Type*—Choose STS.
- *Size*—Choose STS-1.
- *Bidirectional*—Deselect for this circuit.
- *Number of circuits*—Leave the default unchanged (1).
- *Auto-ranged*—Unavailable when *Number of Circuits* is 1.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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, and VT tunnels, Ethergroup sources, and drops are unavailable.

- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Choose 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 choose this box, CTC only displays protected cards as source and destination choices.

Figure 6-8 Setting circuit attributes for a unidirectional DS-3 circuit



Circuit Creation

Circuit Attributes

Circuit

Name: Unidirectional DS3

Type: STS

Size: STS-1

□ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Complete the "DLP-208 Provision a DS-3 Circuit Source and Destination" task on page 6-27.

Step 8 Deselect **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 10. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 11.

Caution Circuits routed on PCA are not protected. They are pre-empted during BLSR ring and span switches.

Step 10 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 11 Click **Next**. Beneath Route Review and Edit, node icons are displayed 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 12 Complete the "DLP-96 Provision a DS-1 or DS-3 Circuit Route" task on page 6-28 for the DS-3 you are creating.

Step 13 Click **Finish**. After completing the circuit, CTC displays the Circuits window.

Step 14 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 15 Click **Edit**. The Edit Circuit window is displayed with the General tab selected. All nodes in the DCC network are displayed on the network map. Circuit source and destination information appears under the source and destination nodes. To display 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 16 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops is displayed.

Step 17 Click **Create**.

Step 18 On 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 pull-down menus. The card selected in Step b determines whether port, STS, or both display. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

   - If the original circuit was routed on a protected path, you can change the nodal diversity options: [Required, Desired, Don't Care; Link Diverse only]. See Step Step 9 for options descriptions.
   - If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 9 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 19 If you need to create additional drops for the circuit, repeat Steps 17–18 to create the additional drops.

Step 20 Click **Close**. The Circuits window displays.

Step 21 Verify that the new drops are displayed under the Destination column for the circuit you edited. If they do not appear, repeat this procedure, making sure all options are provisioned correctly.

Step 22 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

DLP-218 Provision UPSR Selectors During Circuit Creation

Purpose	Use this task to provision UPSR selectors during circuit creation. Use this task only if the circuit will be routed on a UPSR.
Tools/Equipment	None
Prerequisite Procedures	You must have the Circuit Creation wizard displayed.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Attributes panel of the Circuit Creation wizard, set the UPSR path selectors:

- *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, choose the reversion time. Click the *Reversion time* field and choose a reversion time from the pull-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 UPSR path-level signal failure bit error rate (BER) thresholds. Unavailable for VT circuits.
- *SD threshold*—For STS circuits, set the UPSR 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 Finish the circuit creation procedure that referred you to this task.

DLP-208 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	You perform this task during one of the following procedures: NTP-131 Create an Automatically Routed DS-3 Circuit, page 6-17, or NTP-132 Create a Manually Routed DS-3 Circuit, page 6-21, or NTP-56 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 6-23
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 pull-down menu, choose the node where the source will originate.

Step 2 From the Slot pull-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 pull-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 UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1–3 to define the secondary source. If you do not need to create a secondary source, proceed to Step 6.

Step 5 Click **Next**.

Step 6 From the Node pull-down menu, choose the destination (termination) node.

Step 7 From the Slot pull-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 sub-menus that display based on the card selected in Step 3. See Table 6-2 on page 6-3 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 will receive a Path in Use error and be 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 UPSR bridge/selector circuit exit point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 7–8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Finish the circuit creation procedure that referred you to this task.

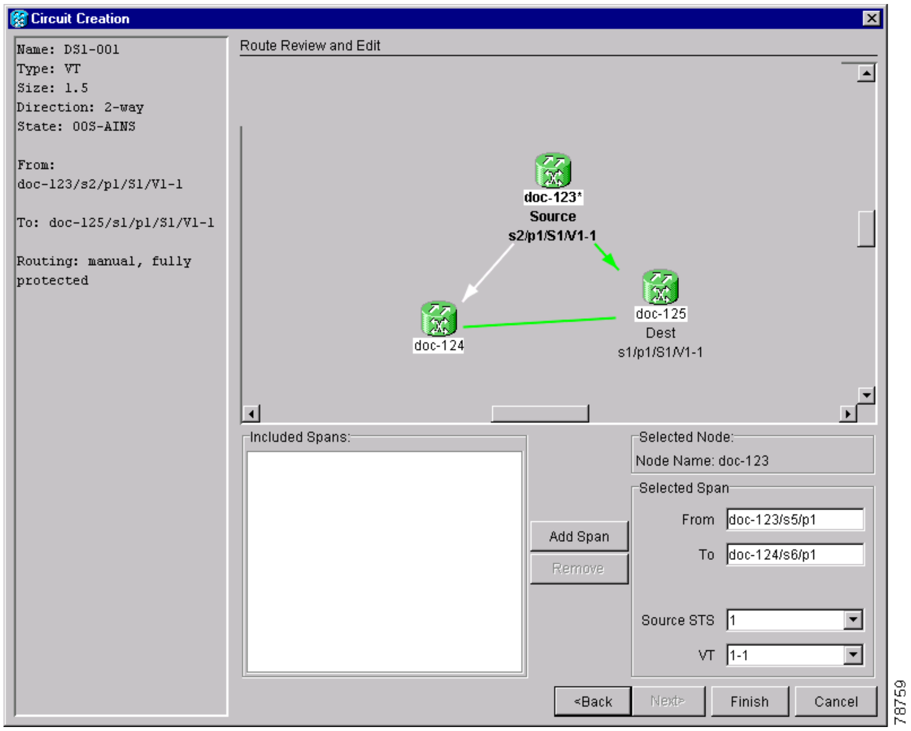
DLP-96 Provision a DS-1 or DS-3 Circuit Route

Purpose	This task provisions the circuit route for DS-1 or DS-3 manually-routed circuits.
Tools/Equipment	None
Prerequisite Procedures	You perform this task during one of the following procedures: NTP-128 Create an Automatically Routed DS-1 Circuit, page 6-6, or NTP-129 Create a Manually Routed DS-1 Circuit, page 6-10, or NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12 NTP-131 Create an Automatically Routed DS-3 Circuit, page 6-17, or NTP-132 Create a Manually Routed DS-3 Circuit, page 6-21, or NTP-56 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 6-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard under Route Review and Edit, 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. Beneath Selected Span, the *From* and *To* fields display span information. The source STS and VT (DS-1 circuit only) are displayed. Figure 6-9 shows a DS-1 circuit example.

Figure 6-9 Manually routing a DS-1 circuit



```
Name: DS1-001
Type: VT
Size: 1.5
Direction: 2-way
State: OOS-AINS

From:
doc-123/s2/p1/S1/V1-1

To: doc-125/s1/p1/S1/V1-1

Routing: manual, fully
protected
```

Selected Node: Node Name: doc-123

Selected Span: From doc-123/s5/p1; To doc-124/s6/p1; Source STS 1; VT 1-1

Step 3 If you want to change the source STS, adjust the *Source STS* field; otherwise, proceed to Step 4.

Step 4 If you want to change the source VT for DS-1 circuits, adjust the *Source VT* field; otherwise, proceed to Step 5.

Note VT is grey (unavailable) for DS-3 circuits.

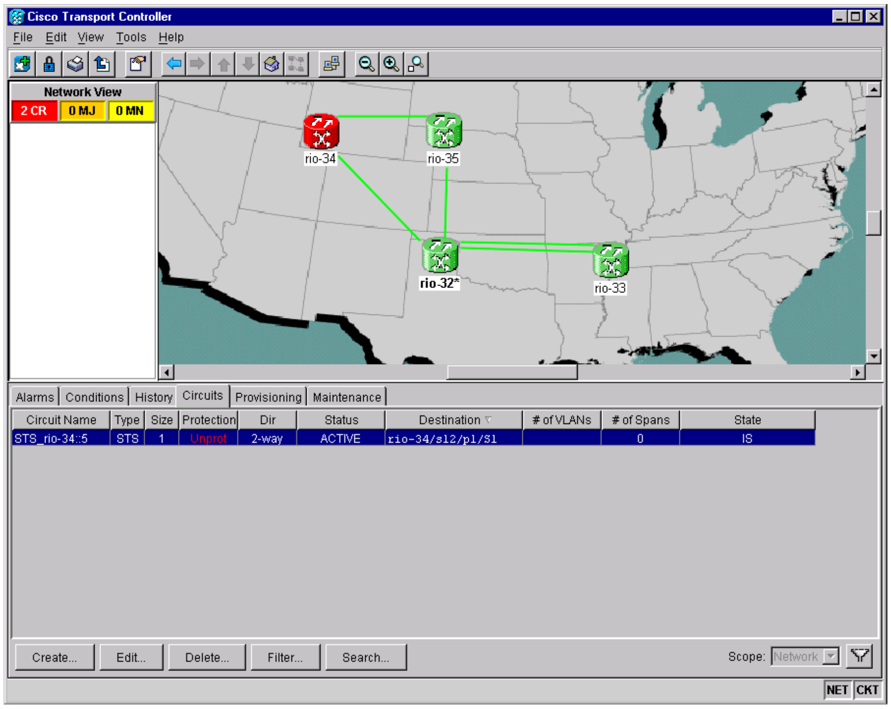
Step 5 Click **Add Span**.The span is added to the Included Spans list and the span arrow turns blue.

Repeat Steps 2–5 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 UPSR 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

Figure 6-10 shows an example of a fully protected circuit routed from a UPSR node to a BLSR node. In the example, the RIO-32, RIO-34, and RIO-35 nodes reside in a BLSR. A UPSR subtends from RIO-32 to RIO-33. To create a circuit from RIO-33 to RIO-35, two spans must be included in the circuit route from RIO-32 to RIO-33, since both the working and protect path must be provisioned for the UPSR portion of the circuit, and one span is included from RIO-32 to RIO-35, since the BLSR provides protection.

Figure 6-10 Manually routing a DS-1 circuit



Circuit Name	Type	Size	Protection	Dir	Status	Destination	# of VLANs	# of Spans	State
STS_rio-34::5	STS	1	Unprot	2-way	ACTIVE	rio-34/s12/p1/S1		0	IS

Step 6 Finish the circuit creation procedure that referred you to this task.

NTP-133 Create an Automatically Routed VT Tunnel

Purpose	This procedure creates an automatically routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through 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 Circuits and Tunnels chapter in the *Cisco ONS 15454 Reference Guide* for more information.

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

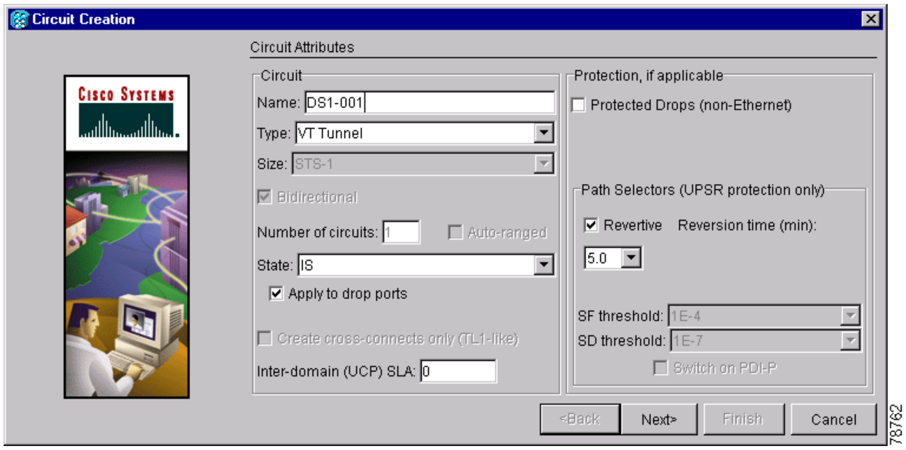
Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab, then click **Create**.

Step 4 In the Circuit Creation dialog box (Figure 6-1), complete the following fields:

- *Name*—Assign a name to the VT tunnel. 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 tunnel.
- *Type*—Choose VT Tunnel. The Bidirectional, Number of Circuits, and Create Cross Connects fields in the dialog box become unavailable.
- *Size*—Unavailable for VT tunnels.
- *Bidirectional*—Unavailable for VT tunnels.
- *Number of circuits*—Unavailable for VT tunnels.
- *Auto-ranged*—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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *Apply to drop ports*—Uncheck this box.
- *Inter-domain (UCP) SLA*—If the tunnel will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Figure 6-11 Setting attributes for a VT tunnel



Circuit Creation

Circuit Attributes

Circuit

Name: DS1-001

Type: VT Tunnel

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 Click **Next**.

Step 6 Beneath Circuit Source, choose the node where the VT tunnel will originate from the Node pull-down menu.

Step 7 Click **Next**.

Step 8 Beneath Circuit Destination, choose the node where the VT tunnel will terminate from the Node pull-down menu.

Step 9 Click **Next**.

Step 10 Beneath Circuit Routing Preferences, choose **Route Automatically**. The following options are available:

- *Using Required Nodes/Spans*—Choose this box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.
- *Review Route Before Creation*—Choose this box to review and edit the VT tunnel route before the circuit is created.

Choose either, both, or none, based on your preferences

Step 11 If you selected Using Required Nodes/Spans:

a. Click **Next**.

b. Beneath Circuit Route Constraints, 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/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 under 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 12 If you selected Review Route Before Creation:

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 13 Click **Finish**. The Circuits window displays.

Step 14 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

NTP-134 Create a Manually Routed VT Tunnel

Purpose	This procedure creates a manually routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through 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 Circuits and Tunnels chapter in the *Cisco ONS 15454 Reference Guide* for more information.

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

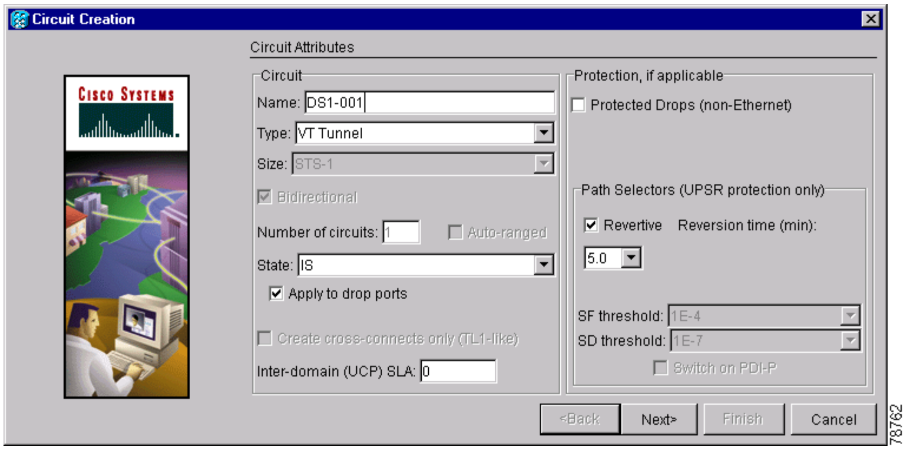
Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab, then click **Create**.

Step 4 In the Circuit Creation dialog box (Figure 6-12), complete the following fields:

- *Name*—Assign a name to the VT tunnel. 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 tunnel.
- *Type*—Choose VT Tunnel. The Bidirectional, Number of Circuits, and Create Cross Connects fields in the dialog box become unavailable (greyed out).
- *Size*—Unavailable for VT tunnels.
- *Bidirectional*—Unavailable for VT tunnels.
- *Number of circuits*—Unavailable for VT tunnels.
- *Auto-ranged*—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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *Apply to drop ports*—Uncheck this box.
  - Inter-domain (UCP) SLA—If the tunnel will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Figure 6-12 Setting attributes for a VT tunnel



Circuit Creation

Circuit Attributes

Circuit

Name: DS1-001

Type: VT Tunnel

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 Click **Next**.

Step 6 Beneath Circuit Source, choose the node where the VT tunnel will originate from the Node pull-down menu.

Step 7 Click **Next**.

Step 8 Beneath Circuit Destination, choose the node where the VT tunnel will terminate from the Node pull-down menu.

Step 9 Click **Next**.

Step 10 Beneath Circuit Routing Preferences, deselect **Route Automatically**.

Step 11 Click **Next**. Beneath Route Review and Edit, node icons are displayed to 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 12 Complete the "DLP-219 Provision a VT Tunnel Route" task on page 6-35 for the tunnel you are creating. The Circuits window displays.

Step 13 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

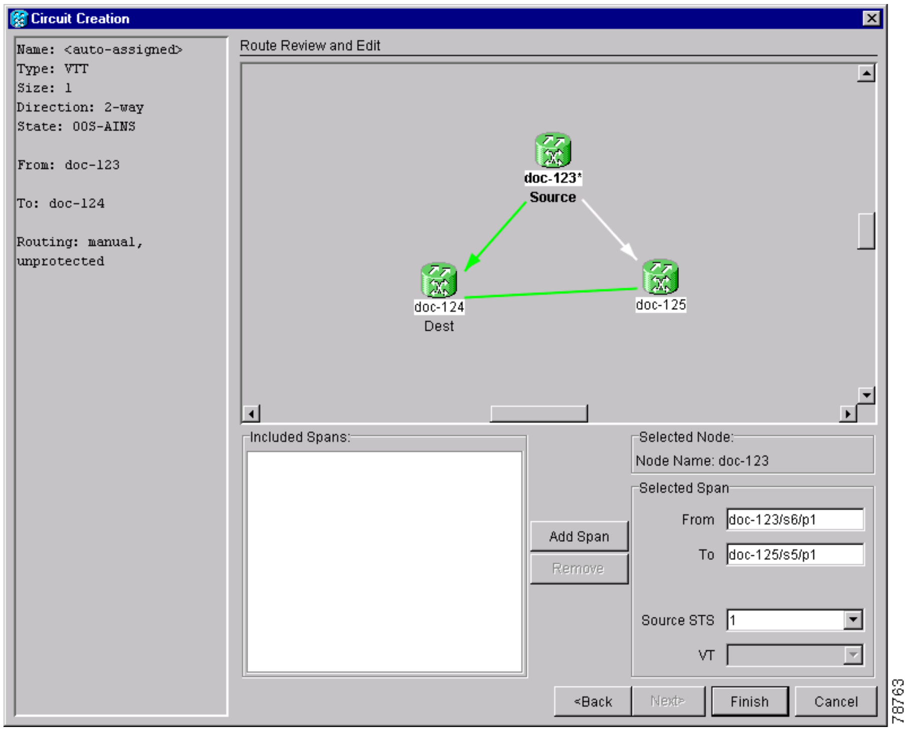
DLP-219 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually-routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	Perform this task as part of the "NTP-134 Create a Manually Routed VT Tunnel" procedure on page 6-33.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard under Route Review and Edit, 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. Beneath Selected Span, the *From* and *To* fields display the slot and port that will carry the tunnel. The source STS is displayed. Figure 6-13 shows an example.

Figure 6-13 Manually routing a VT tunnel



```
Name: <auto-assigned>
Type: VTT
Size: 1
Direction: 2-way
State: OOS-AINS

From: doc-123

To: doc-124

Routing: manual,
unprotected
```

Selected Node:
Node Name: doc-123

Selected Span
From: doc-123/s6/p1
To: doc-125/s5/p1
Source STS: 1
VT:

Step 3 If you want to change the source STS, change it in the *Source STS* field; otherwise, proceed to 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 3–4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Return to the "NTP-134 Create a Manually Routed VT Tunnel" procedure on page 6-33.

NTP-135 Test Electrical Circuits

Purpose	Use this procedure to test DS-1 and DS-3 circuits.
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-128 Create an Automatically Routed DS-1 Circuit, page 6-6 NTP-129 Create a Manually Routed DS-1 Circuit, page 6-10 NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 6-12 NTP-131 Create an Automatically Routed DS-3 Circuit, page 6-17 NTP-132 Create a Manually Routed DS-3 Circuit, page 6-21 NTP-56 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 6-23
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuit** 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.** On the Set Circuit State dialog box, choose **OOS-MT** from the Target State pull-down menu.
- **c.** Check the **Apply to drop ports** checkbox.
- **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 pull-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. – 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) to the test set receive (RX). 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 transmit (TX) to the receive (RX) 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 transmit (TX) to the test set receive (RX). 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: (transmit (TX) port of the test set to the circuit receive (RX) port; test set receive (RX) port to the circuit transmit (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 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. After you choose muxed DS-3, choose the DS-1 to test on the muxed 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 displays a clean signal. If a clean signal is not displayed, repeat Steps 1–8 to make sure the test set and cabling is configured correctly.

Step 10 Inject errors from the test set. Verify that the errors display at the source and destination nodes.

Step 11 Clear the PMs for the ports that you tested. See the "DLP-130 Clear Selected PM Counts" task on page 8-16 for instructions.

Step 12 Put the circuit and circuit ports back 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. On the Set Circuit State dialog box, choose **IS** (in service), **OOS** (out of service) or **OOS-AINS** (auto in service) from the Target State pull-down menu.

c. Check the **Apply to drop ports** checkbox.

d. Click **Apply**.

Step 13 Perform the protection switch test appropriate to the SONET topology:

- For UPSRs, complete the "DLP-94 UPSR Protection Switching Test" task on page 5-35
- For BLSRs complete the "DLP-91 BLSR Ring Switch Test" task on page 5-24.

Step 14 Perform a Bit Error Rate Test (BERT) for 12 hours or a duration dictated by local testing custom. 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.

NTP-136 Create an Automatically Routed Optical Circuit

Purpose	This procedure creates an automatically-routed bidirectional or unidirectional optical circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c speeds.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-1), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the optical 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).
- *Number of circuits*—Type the number of optical 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 checkbox is automatically selected when you enter more than 1 in the *Number of circuits* field. Leave selected if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Deselect the box if you do not want CTC to create the circuits automatically.
- *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—(default) The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).

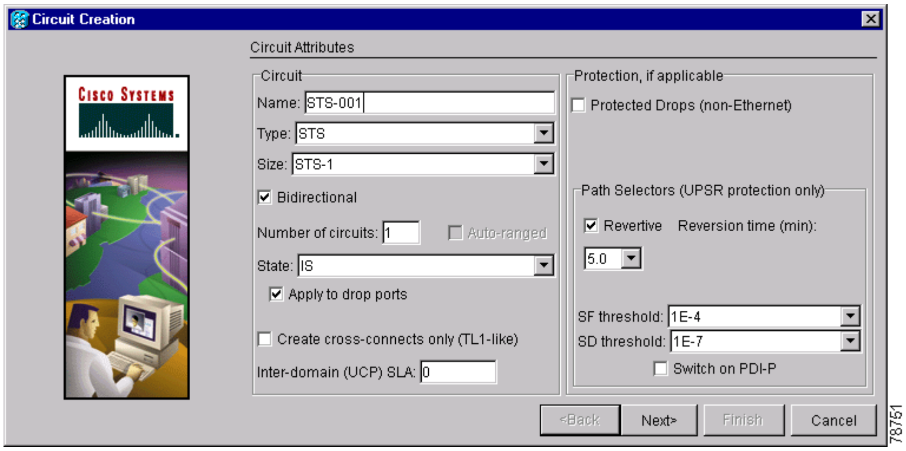
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-230 Change a Circuit State" task on page 9-7.

- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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 and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Choose this 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 choose this box, CTC only displays protected cards as source and destination choices.

Figure 6-14 Setting circuit attributes for an optical circuit


Circuit Creation

Circuit Attributes

Circuit

Name: STS-001

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Complete the "DLP-97 Provision an Optical Circuit Source and Destination" task on page 6-47 for the optical circuit you are creating.

Step 8 Beneath Circuit Routing Preferences (Figure 6-15 on page 6-40), choose **Route Automatically**. The following options are available:

- *Using Required Nodes/Spans*—Choose this checkbox to specify nodes and spans to include or exclude in the CTC-generated circuit route.

- *Review Route Before Creation*—Choose this checkbox to review and edit the circuit route before the circuit is created.

Choose either, both, or none, based on your preferences.

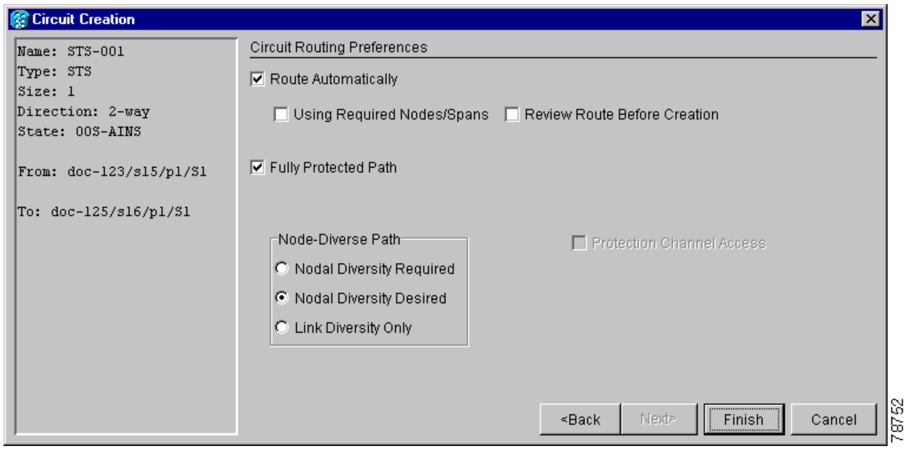
Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 10. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 11.

Step 10 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 6-15 Setting circuit routing preferences for an optical circuit



Circuit Creation

Name: STS-001
Type: STS
Size: 1
Direction: 2-way
State: OOS-AINS

From: doc-123/s15/p1/S1

To: doc-125/s16/p1/S1

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path

○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access

Step 11 If you selected **Using Required Nodes/Spans** complete the following substeps. If not, proceed to Step 12:

a. Click **Next**.

b. Beneath Circuit Route Constraints, 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 will be 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 under 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 12 If you selected Review Route Before Creation, complete the following substeps; otherwise, proceed to Step 13:

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-137 Create a Manually Routed Optical Circuit" procedure on page 6-41 to assign the circuit route yourself.

Step 13 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 *Number of circuits* 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 is displayed. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in *Number of circuits* and did not choose *Auto-ranged*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat Steps Step 4–13 for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 14 On the Circuits window, verify that the circuit(s) you created appear in the circuits list.

Step 15 Complete the "NTP-62 Test Optical Circuits" procedure on page 6-50. Skip this step if you built a test circuit.

NTP-137 Create a Manually Routed Optical Circuit

Purpose	This procedure creates a manually-routed, bidirectional or unidirectional optical circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c speeds.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 In the Circuit Creation dialog box, complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the optical 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).
- *Number of circuits*—Type the number of optical circuits you want to create. The default is 1.
- *Auto-ranged*—Applies to automatically-routed circuits only. If you entered more than 1 in *Number of Circuits*, deselect this box. (The box is unavailable if only one circuit is entered in *Number of Circuits*.)
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

  Note LOS alarms display 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 and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Choose 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 choose this box, CTC only displays protected cards as source and destination choices.

Step 4 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 5 Click **Next**.

Step 6 Complete the "DLP-97 Provision an Optical Circuit Source and Destination" task on page 6-47 for the optical circuit you are creating.

Step 7 Beneath Circuit Routing Preferences (Figure 6-15 on page 6-40), deselect **Route Automatically**.

Step 8 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 9.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 10.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 10.

⚠ **Caution** Circuits routed on PCA are not protected and are pre-empted during BLSR ring and span switches.

Step 9 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 10 Click **Next**. Beneath Route Review and Edit, node icons are displayed so you can route the circuit manually.

Step 11 Complete the "DLP-98 Provision an Optical Circuit Route" task on page 6-48.

Step 12 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 *Number of circuits*, the Circuit Creation dialog box is displayed after the circuit is created so you can create the remaining circuits. Repeat Steps 3–12 for each additional circuit.

Step 13 When all the circuits are created, CTC displays the main Circuits window. Verify that the circuit(s) you created appear in the window.

Step 14 Complete the "NTP-62 Test Optical Circuits" procedure on page 6-50.

NTP-138 Create a Unidirectional Optical Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional OC-N circuit with multiple traffic drops (circuit destinations)
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the node where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. The default (node) view displays.

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, complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the circuit size: STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, or STS-192c.
- *Bidirectional*—Deselect this checkbox for this circuit.
- *Number of circuits*—Leave the default unchanged (1).
- *Auto-ranged*—Unavailable when *Number of Circuits* is 1.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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 and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Choose 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 choose this box, CTC only displays protected cards as source and destination choices.

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Complete the "DLP-97 Provision an Optical Circuit Source and Destination" task on page 6-47 for the circuit you are creating.

Step 8 Deselect **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and proceed to Step 10. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and proceed to Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, then proceed to Step 11.

Caution Circuits routed on PCA are not protected. They are pre-empted during BLSR ring and span switches.

Step 10 If you selected Fully Protected Path, choose one of the following:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- *Nodal Diversity Desired*—(default) Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the UPSR portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may 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 11 Click **Next**. Beneath Route Review and Edit, node icons are displayed 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 12 Complete the "DLP-98 Provision an Optical Circuit Route" task on page 6-48.

Step 13 Click **Finish**. After completing the circuit, CTC displays the Circuits window.

Step 14 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 15 Click **Edit**. The Edit Circuit window is displayed with the General tab selected. All nodes in the DCC network are displayed on the network. Circuit source and destination information appears under the source and destination nodes. To display 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, pressing **Ctrl** and dragging the icon to the new location.

Step 16 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops is displayed.

Step 17 Click **Create**.

Step 18 On 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 pull-down menus. The choice in these menus depends on the card selected in Step b. See Table 6-2 on page 6-3 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

  - If the original circuit was routed on a protected path, you can change the nodal diversity options: Required, Desired, Don't Care; Link Diverse only. See Step 10 for options descriptions.
  - If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 11 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 19 If you need to create additional drops on the circuit, repeat Steps 16–18.

Step 20 Click **Close**. The Circuits window appears.

Step 21 Verify that the new drops are displayed under the Destination column for the circuit you edited. If they do not appear, repeat Steps 17–20 making sure all options are provisioned correctly.

Step 22 Complete the "NTP-62 Test Optical Circuits" procedure on page 6-50.

DLP-97 Provision an Optical Circuit Source and Destination

Purpose	This task provisions the source and destination cards for an optical circuit.
Tools/Equipment	None
Prerequisite Procedures	Perform this task during one of the following procedures: NTP-136 Create an Automatically Routed Optical Circuit, page 6-38 NTP-137 Create a Manually Routed Optical Circuit, page 6-41 NTP-138 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node pull-down menu, choose the node where the circuit will originate.

Step 2 From the Slot pull-down menu, choose the slot containing the optical 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 sub-menus. The Port menu is only available if the card has multiple ports. STSs are not displayed if they are already in use by other circuits.

Note The STSs that display 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 UPSR, 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 UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1–3 to define the secondary source.

Step 5 Click **Next**.

Step 6 From the Node pull-down menu, choose the destination node.

Step 7 From the Slot pull-down menu, choose the slot containing the optical 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 sub-menus. The Port menu is available only if the card has multiple ports. The STSs that display depend on the card, circuit size, and protection scheme.

Step 9 If you need to create a secondary destination, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 6–8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

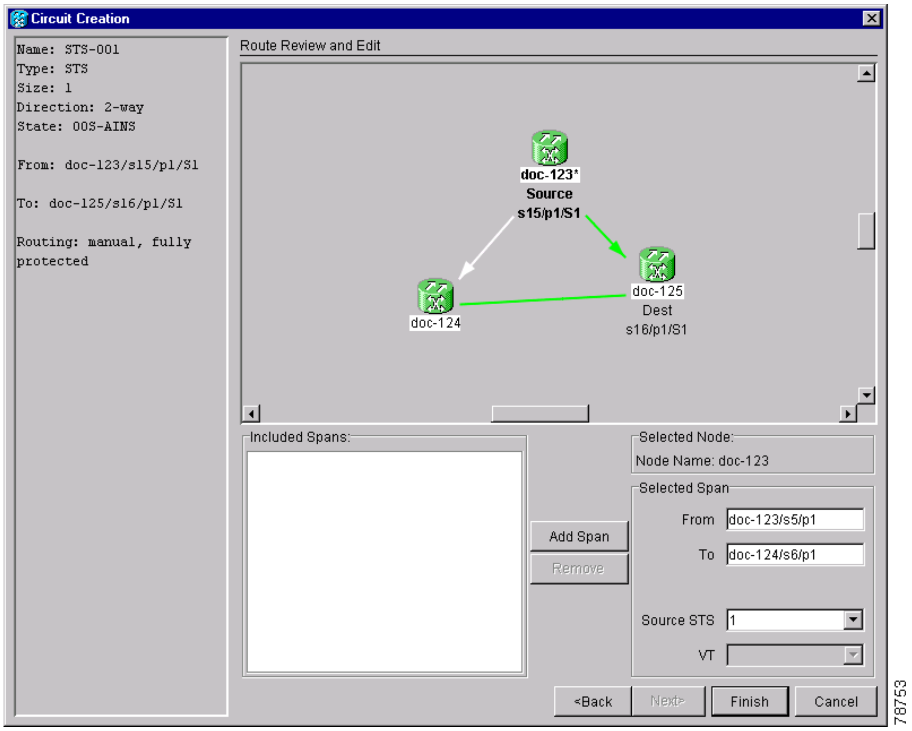
DLP-98 Provision an Optical Circuit Route

Purpose	This task provisions an optical circuit route for manually-routed circuits.
Tools/Equipment	None
Prerequisite Procedures	Perform this task during one of the following procedures: NTP-136 Create an Automatically Routed Optical Circuit, page 6-38 NTP-137 Create a Manually Routed Optical Circuit, page 6-41 NTP-138 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard under Route Review and Edit, 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. Beneath Selected Span, the *From* and *To* fields display span information. The source STS is displayed. Figure 6-16 shows an example.

Figure 6-16 Manually routing a OC-N circuit



Circuit Creation

```
Name: STS-001
Type: STS
Size: 1
Direction: 2-way
State: OOS-AINS

From: doc-123/s15/p1/S1

To: doc-125/s16/p1/S1

Routing: manual, fully
protected
```

Route Review and Edit

Selected Node:
Node Name: doc-123

Selected Span
From doc-123/s5/p1
To doc-124/s6/p1
Source STS 1
VT

Step 3 If you want to change the source STS, adjust the *Source STS* field; otherwise, proceed to the next step.

Note VT is grey for OC-N circuits.

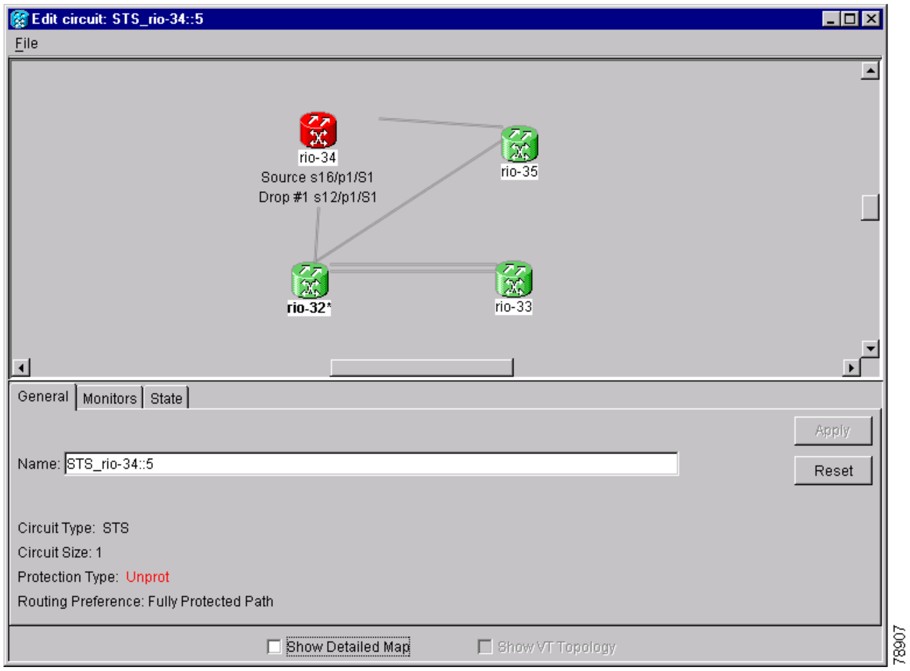
Step 4 Click **Add Span**.The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 2–4 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 UPSR 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

Figure 6-17 shows an example of a fully protected circuit routed from a UPSR node to a BLSR node. In the example, RIO-32, RIO-34, and RIO-35 reside in a BLSR. A UPSR subtends from RIO-32 to RIO-33. To create a circuit from RIO-33 to RIO-35, two spans must be included in the circuit route from RIO-32 to RIO-33, since both working and protect path must be provisioned for the UPSR portion of the circuit, and one span is included from RIO-32 to RIO-35, since the BLSR provides protection.

Figure 6-17 Routing an OC-N circuit from a subtending ring



Name: STS_rio-34::5

Circuit Type: STS
Circuit Size: 1
Protection Type: Unprot
Routing Preference: Fully Protected Path

Step 6 Finish the circuit creation procedure that referred you to this task.

NTP-62 Test Optical Circuits

Note If this has not been done, do so now before completing the optical circuit test procedure.

Purpose	Use this procedure to test an optical circuit.
Tools/Equipment	Test set capable of optical 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-136 Create an Automatically Routed Optical Circuit, page 6-38 NTP-137 Create a Manually Routed Optical Circuit, page 6-41
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into the node where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

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 Out of Service-Maintenance (OOS_MT):

a. Click the circuit you want to test.

b. From the Tools menu, choose **Circuits > Set Circuit State**.

c. On the Set Circuit State dialog box, choose **OOS-MT** from the Target State pull-down menu.

d. If unchecked, check the **Apply to drop ports** checkbox.

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 transmit (TX) to the receive (RX) 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 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. At the source node attach the loopback cable to the port you are testing. Connect the test set to the circuit source port: transmit (TX) port of the test set to the circuit receive (RX) port; test set receive (RX) port to the circuit transmit (TX) port.

Step 7 Configure the test set for the source ONS 15454 card:

- *OC-3 cards*—You will test either an OC-3c (the "c" denotes concatenated) or a muxed OC-3. If you are testing an OC-3c, configure the test set for an OC-3c. If you are testing a muxed OC-3, configure the test set for a muxed 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 muxed OC-12. If you are testing an OC-12c, configure the test set for an OC-12c. If you are testing a muxed OC-12, configure the test set for a muxed OC12 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 muxed OC-48. If you are testing an OC-48c configure the test set for an OC-48c. If you are testing a muxed OC-48, configure the test set for a muxed 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 muxed OC-192. If you are testing an OC-192c configure the test set for an OC-192c. If you are testing a muxed OC-192, configure the test set for a muxed 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 displays a clean signal. If a clean signal is not displayed, repeat Steps 1–7 to make sure you have configured the test set and cabling.

Step 9 Inject errors from the test set. Verify that the errors display at the source and destination nodes.

Step 10 Clear the PMs for the ports that you tested. See the "DLP-130 Clear Selected PM Counts" task on page 8-16 for instructions.

Step 11 Perform protection switch testing appropriate to SONET topology:

- For UPSRs, see the "DLP-94 UPSR Protection Switching Test" task on page 5-35.
- For BLSRs see the "DLP-91 BLSR Ring Switch Test" task on page 5-24.

Step 12 Perform a Bit Error Rate Test (BERT) for 12 hours or a duration dictated by local testing custom. For information about configuring your test set for 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. On the Set Circuit State dialog box, choose **IS** (in service), **OOS**, (out of service) or **OOS-AINS** (auto inservice) from the Target State pull-down menu.

c. If unchecked, check the **Apply to drop ports** checkbox.

d. Click **Apply**.

NTP-139 Create a Half Circuit on a BLSR or 1+1 Node

Purpose	Use this procedure to create a DS1, DS3, or OC-N circuit from a drop to an OC-N line card on the same node in a BLSR or 1+1 topology.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the half circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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, complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *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.
- *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).
- *Number of circuits*—Type the number of circuits you want to create. The default is 1.
- *Auto-ranged*—This checkbox is automatically selected if you enter more than 1 in the *Number of circuits* field. Deselect the box.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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 and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Deselect this box.

Step 5 Click **Next**.

Step 6 Provision the circuit source:

a. From the Node pull-down menu, choose the node that will contain the circuit.

b. From the Slot pull-down menu, choose the slot containing the card where the circuit will originate.

c. From the Port pull-down menu, choose the port where the circuit will originate. This field will not be available if a DS-1 card is chosen in Step b.

d. 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 pull-down menu.

Step 7 Click **Next**.

Step 8 Provision the circuit destination:

a. From the Node pull-down menu, choose the node chosen in Step 6a.

b. From the Slot pull-down menu, choose the OC-N card to map the DS-1 to a VT1.5 for optical transport or to map the DS-3 or OC-N STS circuit to an STS.

c. Choose the destination STS or VT from the sub-menus that display.

Step 9 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 *Number of circuits* 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 is displayed. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in *Number of circuits* and did not choose *Auto-ranged*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 10 On the Circuits window, verify that the circuit(s) just created appear in the circuits list.

Step 11 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-140 Create a Half Circuit on a UPSR Node

Purpose	Use this procedure to create a DS1, DS3, or OC-N circuit from a drop to an OC-N line card on the same UPSR node.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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, complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *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.
- *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).
- *Number of circuits*—Type the number of circuits you want to create. The default is 1. I
- *Auto-ranged*—This checkbox is automatically selected if you enter more than 1 in the *Number of circuits* field. Deselect the box.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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 and VT tunnels and Ethergroup sources and drops are unavailable.
- *Inter-domain (UCP) SLA*—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave this box unchecked.

Step 5 Set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 6 Click **Next**.

Step 7 Provision the circuit source:

a. From the Node pull-down menu, choose the node that will contain the circuit.

b. From the Slot pull-down menu, choose the slot containing the card where the circuit will terminate.

c. From the Port pull-down menu, choose the port where the circuit will terminate. This field will not be available if a DS-1 card is chosen in Step b.

d. From the DS1 pull-down menu, choose the DS-1 where the traffic will terminate. This field is only available for VT circuits.

Step 8 **Click Next**.

Step 9 Provision the circuit destination:

a. From the Node pull-down menu, choose the node that will contain the circuit. This will be the same as the node chosen in Step 6a.

b. From the Slot pull-down menu, choose the OC-N card to map the DS-1 to a VT1.5 for optical transport or to map the DS-e circuit to an STS.

c. Choose the destination STS or VT from the sub-menus that display.

Step 10 Click **Use Secondary Destination** and repeat Steps 7–9 to define the secondary destination.

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 *Number of circuits* 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 is displayed. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in *Number of circuits* and did not choose *Auto-ranged*, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 12 On the Circuits window, verify that the circuit(s) just created appear in the circuits list.

Step 13 Complete the "NTP-135 Test Electrical Circuits" procedure on page 6-36. Skip this step if you built a test circuit.

NTP-141 Provision an E Series EtherSwitch Circuit (Multicard or Single-Card)

Purpose	This procedure creates a multicard or single-card EtherSwitch Circuit
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-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 If a high number of VLANs is already used by the system, complete the "DLP-99 Determine Available VLANs" task on page 6-71 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 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-246 Provision E Series Ethernet Card Mode" task on page 6-72.

Step 4 From the View menu, choose **Go to Network View**.

Step 5 Click the **Circuits** tab, then click **Create**.

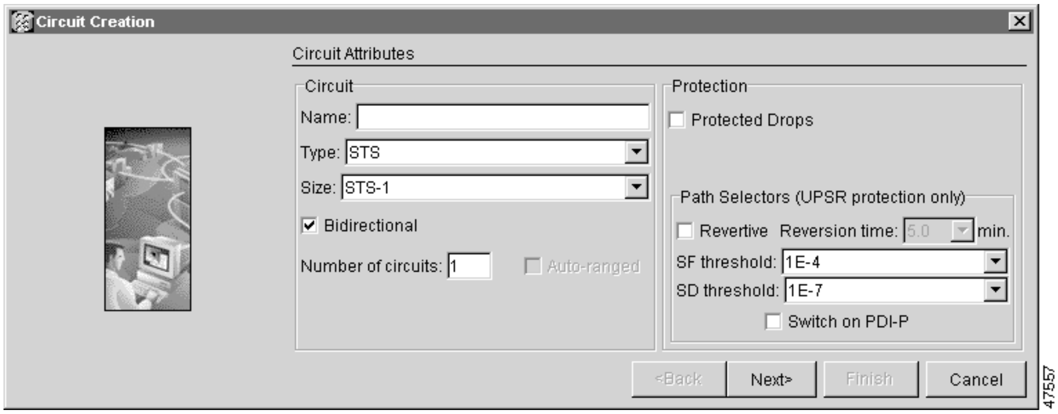
Step 6 In the Create Circuits dialog box (Figure 6-18 on page 6-57), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *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).
- *Number of circuits*—Leave the default unchanged (1).
- *Auto-ranged*—Unavailable.
- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave the default unchanged (unchecked).

Step 7 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Figure 6-18 Provisioning an Ethernet circuit



Circuit Creation

Circuit Attributes

Circuit

Name:

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

Protection

□ Protected Drops

Path Selectors (UPSR protection only)

□ Revertive Reversion time: 5.0 min.

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 8 Click **Next**.

Step 9 Provision the circuit source:

a. From the Node pull-down menu, choose one of the EtherSwitch circuit endpoint nodes. (Either end node can be the EtherSwitch circuit source.)

b. From the Slot pull-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 10 Click **Next**.

Step 11 Provision the circuit destination:

a. From the Node pull-down menu, choose the second EtherSwitch circuit endpoint node.

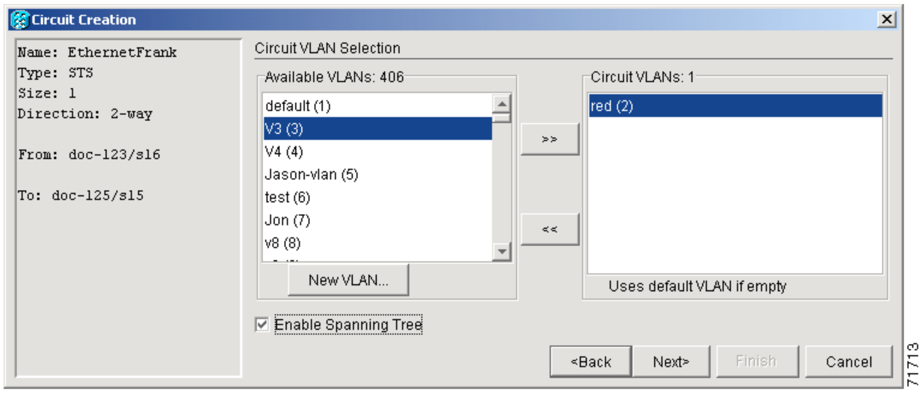
b. From the Slot pull-down menu, choose one of the following:

- 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 12 Click **Next**.

Step 13 Beneath Circuit VLAN Selection (Figure 6-19 on page 6-58), click **New VLAN**. If the desired VLAN already exists, proceed to Step 16.

Figure 6-19 Circuit VLAN selection dialog with Enable Spanning Tree checkbox



```
Name: EthernetFrank
Type: STS
Size: 1
Direction: 2-way

From: doc-123/s16

To: doc-125/s15
```

Available VLANs: 406
- default (1)
- V3 (3)
- V4 (4)
- Jason-vlan (5)
- test (6)
- Jon (7)
- v8 (8)

Circuit VLANs: 1
- red (2)

Uses default VLAN if empty

☑ Enable Spanning Tree

Step 14 In the 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.

Step 15 Click **OK**.

Step 16 Beneath Circuit VLAN Selection, highlight the VLAN name and click the arrow >> button to move the available VLAN(s) to the Circuit VLANs column.

Step 17 If you are building a Single-card EtherSwitch circuit and want to disable spanning tree protection on this circuit, uncheck the **Enable Spanning Tree** checkbox and click **OK** on the Disabling Spanning Tree dialog. The Enable Spanning Tree box will remain 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 will incur blocking if the circuits traverse the same E-series Ethernet card and use the same VLAN.

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 at the card view of CTC under the Provisioning tab.

Step 18 Click **Next**.

Step 19 Confirm that the following information about the circuit is correct:

- Circuit name

- Circuit type
- Circuit size
- ONS 15454 circuit nodes

Step 20 Click **Finish**.

Step 21 Complete the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73.

Step 22 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75.

NTP-142 Create an E Series Shared Packet Ring Ethernet Circuit

Purpose	This procedure creates a shared packet ring Ethernet circuit.
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-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 If a high number of VLANs is already used by the system, complete the "DLP-99 Determine Available VLANs" task on page 6-71 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 Multi-card EtherSwitch Group. See the "DLP-246 Provision E Series Ethernet Card Mode" task on page 6-72.

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:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the circuit size. Valid shared packet ring circuit sizes are STS-1, STS-3c, and STS6c.
- *Bidirectional*—Leave checked for this circuit (default).
- *Number of circuits*—Leave set at 1 (default).
- *Auto-ranged*—Unavailable.
- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave unchecked.

Step 7 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 8 Click **Next**.

Step 9 Provision the circuit source:

a. From the Node pull-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 pull-down menu, choose **Ethergroup**.

Step 10 Click **Next**.

Step 11 Provision the circuit destination:

a. From the Node pull-down menu, choose the second shared packet ring circuit endpoint node.

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

Step 12 Click **Next**.

Step 13 Review the VLANs listed under Available VLANs (Figure 6-20). If the VLAN you want to use is displayed, proceed to Step 14. If you need to create a new VLAN, complete the following steps:

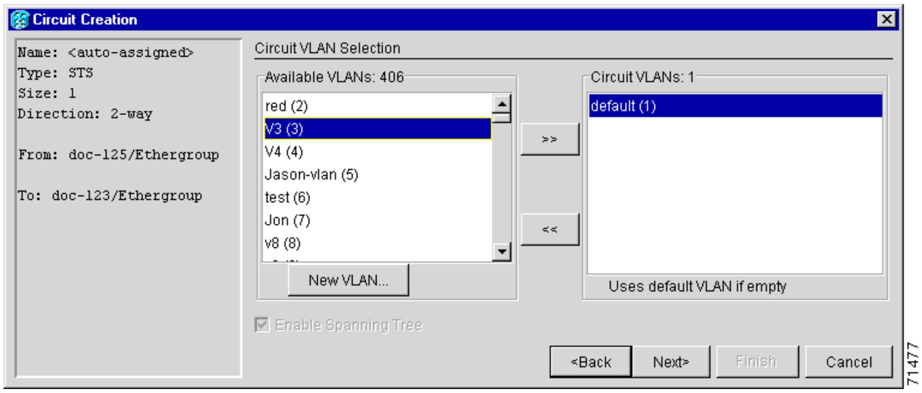
a. Click the **New VLAN** button.

b. On the 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.

c. Click **OK**.

Figure 6-20 Selecting a VLAN



Circuit Creation

```
Name: <auto-assigned>
Type: STS
Size: 1
Direction: 2-way

From: doc-125/Ethergroup

To: doc-123/Ethergroup
```

Circuit VLAN Selection

Available VLANs: 406

- red (2)
- V3 (3)
- V4 (4)
- Jason-vlan (5)
- test (6)
- Jon (7)
- v8 (8)

Circuit VLANs: 1

- default (1)

Uses default VLAN if empty

☑ Enable Spanning Tree

Step 14 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.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

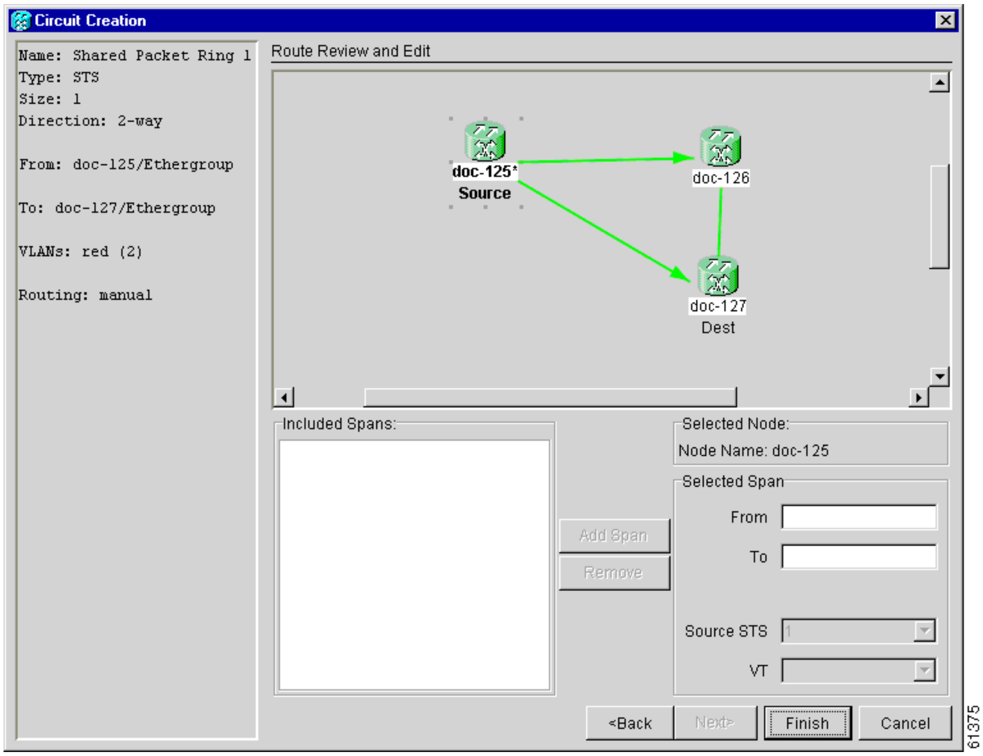
Step 15 Click **Next**.

Step 16 Under Circuit Routing Preferences, uncheck the **Route Automatically** checkbox and click **Next**.

Step 17 Under Route Review and Edit panel (Figure 6-21), click the source node, then click either span (green arrow) leading from the source node.

The span turns white.

Figure 6-21 Adding a span (path)



```
Name: Shared Packet Ring 1
Type: STS
Size: 1
Direction: 2-way

From: doc-125/Ethergroup

To: doc-127/Ethergroup

VLANs: red (2)

Routing: manual
```

Selected Node:
Node Name: doc-125

Source STS 1

Step 18 Click **Add Span**.

The span turns blue. CTC adds the span to the Included Spans list.

Step 19 Click the node at the end of the blue span.

Step 20 Click the green span with the source node from Step 19.

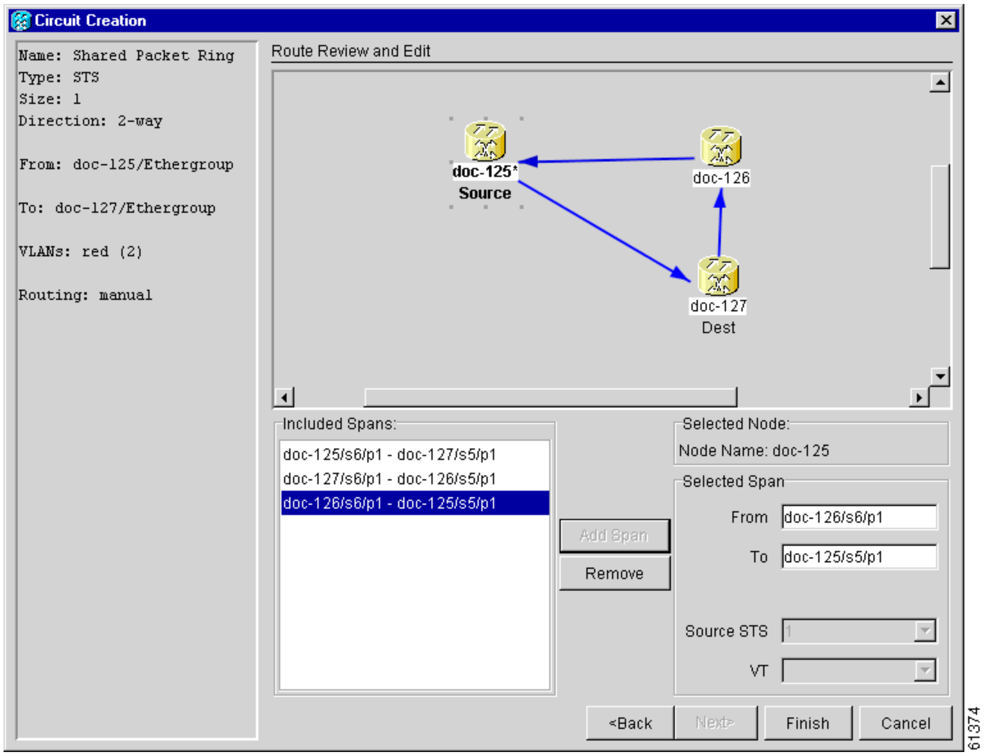
The span turns white.

Step 21 Click **Add Span**.

The span turns blue.

Step 22 Repeat Steps 18–21 for every node in the ring. Figure 6-22 on page 6-62 shows the Circuit Creation dialog box with all the circuit spans selected.

Figure 6-22 Viewing a span (path) after creating an E Series Shared Packet Ring circuit



Circuit Creation

```
Name: Shared Packet Ring
Type: STS
Size: 1
Direction: 2-way

From: doc-125/Ethergroup

To: doc-127/Ethergroup

VLANs: red (2)

Routing: manual
```

Route Review and Edit

Included Spans:
- doc-125/s6/p1 - doc-127/s5/p1
- doc-127/s6/p1 - doc-126/s5/p1
- doc-126/s6/p1 - doc-125/s5/p1

Selected Node:
Node Name: doc-125

Selected Span
From: doc-126/s6/p1
To: doc-125/s5/p1
Source STS: 1
VT:

Step 23 Verify that the new circuit is correctly configured. If the circuit information is not correct, click the **Back** button and repeat the procedure 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 24 Click **Finish**.

Step 25 Complete the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73 for each node that carries the circuit.

Step 26 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75 for each node that carries the circuit.

Step 27 Complete the "NTP-146 Test E Series Ethernet Circuits" procedure on page 6-77.

NTP-143 Create an E Series Hub and Spoke Ethernet Configuration

Purpose	This procedure creates a hub and spoke Ethernet configuration, which is made up of one or more circuits that share a common endpoint.
Tools/Equipment	E Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at all Ethernet circuit end point nodes.
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the hub node (the common endpoint). See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 Complete the "DLP-99 Determine Available VLANs" task on page 6-71 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 Singlecard EtherSwitch Group. See the "DLP-246 Provision E Series Ethernet Card Mode" task on page 6-72.

Step 5 Repeat Steps 3 and 4 for the Ethernet card in the other circuit endpoint. (You only need to verify that the hub node is provisioned for Singlecard EtherSwitch once.)

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the circuit size.
- *Bidirectional*—Leave checked for this circuit (default).
- *Number of circuits*—Leave set at 1 (default).
- *Auto-ranged*—Unavailable.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave unchecked.

Step 8 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

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

b. From the Slot pull-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node pull-down menu, choose an EtherSwitch circuit endpoint node.

b. From the Slot pull-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 13 Click **Next**.

Step 14 Review the VLANs listed under Available VLANs (Figure 6-23). If the VLAN you want to use is displayed, proceed to Step 16. If you need to create a new VLAN, complete the following steps:

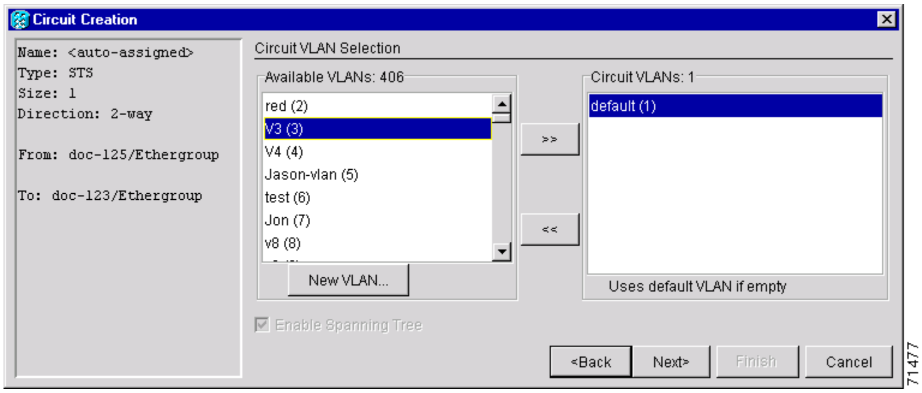
a. Click the **New VLAN** button.

b. On the 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.

c. Click **OK**.

Figure 6-23 Selecting a VLAN



Circuit Creation

```
Name: <auto-assigned>
Type: STS
Size: 1
Direction: 2-way

From: doc-125/Ethergroup

To: doc-123/Ethergroup
```

Circuit VLAN Selection

Available VLANs: 406
red (2)
V3 (3)
V4 (4)
Jason-vlan (5)
test (6)
Jon (7)
v8 (8)

Circuit VLANs: 1
default (1)

Uses default VLAN if empty

☑ Enable Spanning Tree

Step 15 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.

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 16 Click **Next**.

Step 17 Confirm that the following information about the hub and spoke circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15454 circuit nodes

If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information.

Note You can also click **Finish**, delete the completed circuit, and start the procedure from the beginning.

Step 18 Click **Finish**.

Step 19 Complete the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73.

Step 20 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75.

Step 21 Complete the "NTP-146 Test E Series Ethernet Circuits" procedure on page 6-77.

Step 22 To create additional circuits ("spokes"):

a. Complete the "DLP-99 Determine Available VLANs" task on page 6-71 to verify that sufficient VLAN capacity is available for the circuit destination node.

b. Repeat Steps 3 – 21.

NTP-144 Provision 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 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-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
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 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 If a high number of VLANs is already used by the system, complete the "DLP-99 Determine Available VLANs" task on page 6-71 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 On the node view, double-click the Ethernet card that will carry the cross-connect.

Step 4 Verify that the Ethernet cards that will carry the circuit are provisioned for Singlecard EtherSwitch Group. See the "DLP-246 Provision E Series Ethernet Card Mode" task on page 6-72.

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:

- *Name*—Assign a name to the cross-connect. 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 cross-connect.
- *Type*—Choose STS.
- *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 checked for this cross-connect (default).
- *Number of circuits*—Leave set at 1 (default).
- *Auto-ranged*—Unavailable.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.

- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave unchecked.

Step 8 If the circuit will be routed on a UPSR, complete the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

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

b. From the Slot pull-down menu, choose the Ethernet card where you enabled the single-card EtherSwitch in Step 6.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node pull-down menu, choose the cross-connect circuit source node selected in Step 8. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot pull-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 pull-down menus.

Step 13 Click **Next**.

Step 14 Review the VLANs listed under Available VLANs. If the VLAN you want to use is displayed, proceed to Step 15. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the 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.

c. Click **OK**.

Step 15 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 16 Click **Next**. The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 17 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

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 18 Click **Finish**.

Step 19 Complete the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73.

Step 20 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75.

NTP-145 Provision 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-127 Verify Network Turn Up, page 6-4
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 Log into a circuit endpoint. See "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 Complete the "DLP-99 Determine Available VLANs" task on page 6-71 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 multicard EtherSwitch group. See the "DLP-246 Provision E Series Ethernet Card Mode" task on page 6-72.

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:

- *Name*—Assign a name to the source cross-connect. 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 source cross-connect.
- *Type*—Choose STS.

- *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).
- *Number of circuits*—Leave set at 1 (default).
- *Auto-ranged*—Unavailable.
- *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*—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave unchecked.

Step 7 If the circuit will be routed on a UPSR, complete the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 8 Click **Next**.

Step 9 Provision the cross-connect source:

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

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

Step 10 Click **Next**.

Step 11 From the Node pull-down menu under Destination, choose the circuit source node selected in Step 9. (For Ethernet cross-connects, the source and destination nodes are the same.)

The Slot field automatically is provisioned for Ethergroup.

Step 12 Click **Next**.

Step 13 Review the VLANs listed under Available VLANs. If the VLAN you want to use is displayed, proceed to Step 15. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the 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.

c. Click **OK**.

Step 14 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 15 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 16 In the left pane, verify the cross-connect information (in this step, "circuit" refers to the Ethernet cross-connect):

- Circuit name
- Circuit type
- Circuit size
- VLANs
- ONS 15454 nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 17 Click **Finish**.

Step 18 Complete the "DLP-220 Provision E Series Ethernet Ports" task on page 6-73.

Step 19 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75.

Step 20 From the View menu, choose **Go to Home View**.

Step 21 Click the **Circuits** tab.

Step 22 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box opens.

Step 23 Click **Drops** and click **Create**.

The Define New Drop dialog box opens.

Step 24 From the **Slot** menu, choose the OC-N card that links the ONS 15454 to the non-ONS 15454 equipment.

Step 25 From the **Port** menu, choose the appropriate port.

Step 26 From the STS menu, choose the STS that matches the STS of the connecting non-ONS 15454 equipment.

Step 27 Click **OK**.

Step 28 Confirm the circuit information that displays in the Edit Circuit dialog box and click **Close**.

Step 29 Repeat Steps 2–28 at the second ONS 15454 Ethernet manual cross-connect endpoint.

Note The appropriate STS circuit must exist in the non-ONS 15454 equipment to connect the two ONS 15454 Ethernet manual cross-connect endpoints.

Caution If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits may 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 30 Complete the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75.

DLP-99 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.
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-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 At any CTC view, click the **Circuits** tab.

Step 2 Click any existing Ethernet circuit to highlight that row.

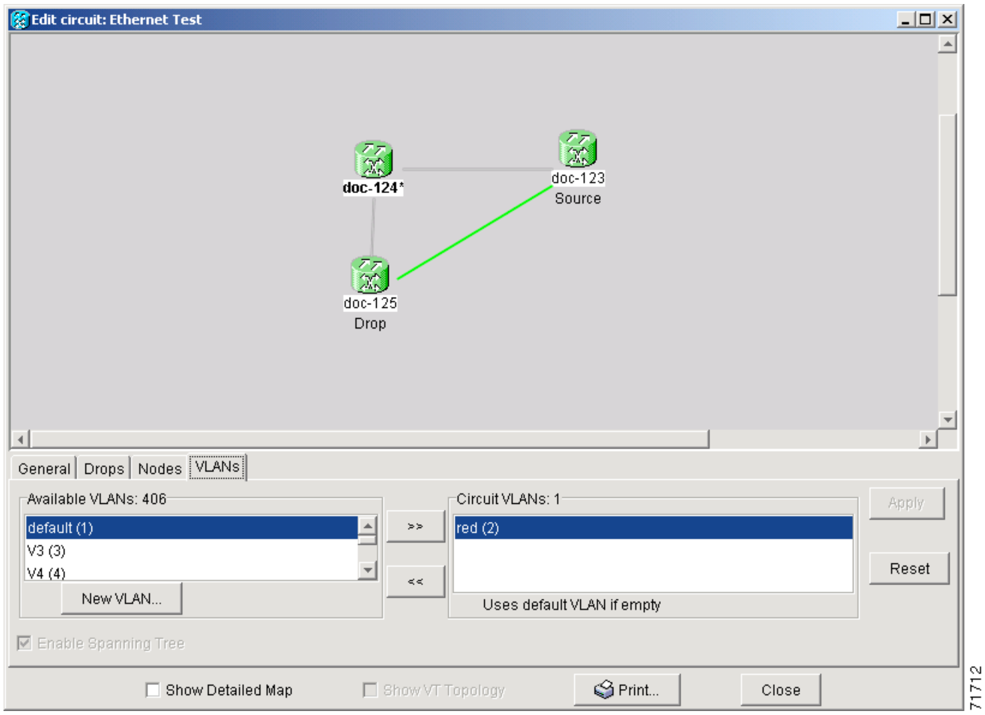
Step 3 Click **Edit**, then click the **VLANs** tab (Figure 6-24 on page 6-72).

The Edit Circuit dialog displays 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 will block each other if the circuits traverse the same E-series Ethernet card and use the same VLAN.

Figure 6-24 Edit Circuit dialog with VLANs tab selected



Step 5 Return to your originating procedure (NTP).

DLP-246 Provision E Series Ethernet Card Mode

Purpose	This task provisions an E Series Ethernet card for either multicard or single-card EtherSwitch circuits
Tools/Equipment	E Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed.
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
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-152 Delete Circuits" procedure on page 9-11.

Step 1 Navigate to 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 Under Card Mode, choose one of the following:

- For Multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group**. Click **Apply**.
- For Single-card EtherSwitch circuits, choose **Single-card EtherSwitch**. Click **Apply**.

Step 4 Multicard EtherSwitch circuits only: repeat Steps 2–3 for all other Ethernet cards in the node that will carry the multicard EtherSwitch circuits.

Step 5 Repeat Steps 1–4 for nodes required by the originating procedure.

Step 6 Return to your originating procedure.

DLP-220 Provision E Series Ethernet Ports

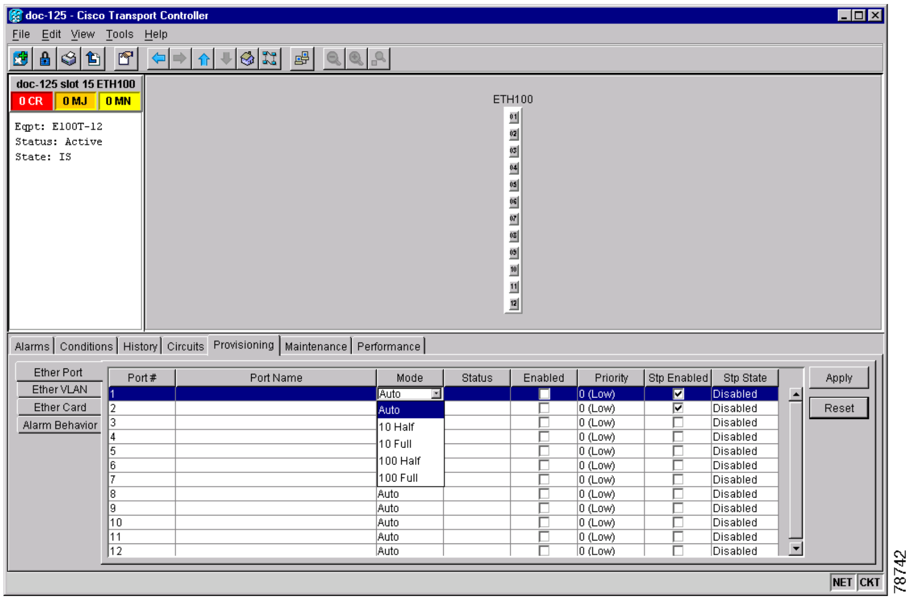
Purpose	This task enables ports for the E100T-12, E100T-G, E1000-2, and E1000-2-G cards.
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required to enable Ethernet traffic
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

Step 1 Display the node view.

Step 2 Double-click the Ethernet card that you want to provision.

Step 3 Click the **Provisioning** > **Ether Port** tabs (Figure 6-25).

Figure 6-25 Provisioning E-100 Series Ethernet ports



Eqpt: E100T-12
Status: Active
State: IS

Port #	Port Name	Mode	Status	Enabled	Priority	Stp Enabled	Stp State
1		Auto		☐	0 (Low)	☑	Disabled
2				☐	0 (Low)	☑	Disabled
3				☐	0 (Low)	☐	Disabled
4				☐	0 (Low)	☐	Disabled
5				☐	0 (Low)	☐	Disabled
6				☐	0 (Low)	☐	Disabled
7				☐	0 (Low)	☐	Disabled
8		Auto		☐	0 (Low)	☐	Disabled
9		Auto		☐	0 (Low)	☐	Disabled
10		Auto		☐	0 (Low)	☐	Disabled
11		Auto		☐	0 (Low)	☐	Disabled
12		Auto		☐	0 (Low)	☐	Disabled

Step 4 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 auto-negotiate 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*—Click this checkbox 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.
- *Stp Enabled*—Click this checkbox to enable the spanning tree protocol (STP) on the port. Refer to the spanning tree information in the Cisco ONS 15454 Reference Manual.

Step 5 Click **Apply**.

Step 6 Repeat Steps 1–5 for all other cards that will be in the VLAN.

Step 7 Your Ethernet ports are provisioned and ready to be configured for VLAN membership.See the "DLP-221 Provision E Series Ethernet Ports for VLAN Membership" task on page 6-75 for instructions.

DLP-221 Provision E Series Ethernet Ports for VLAN Membership

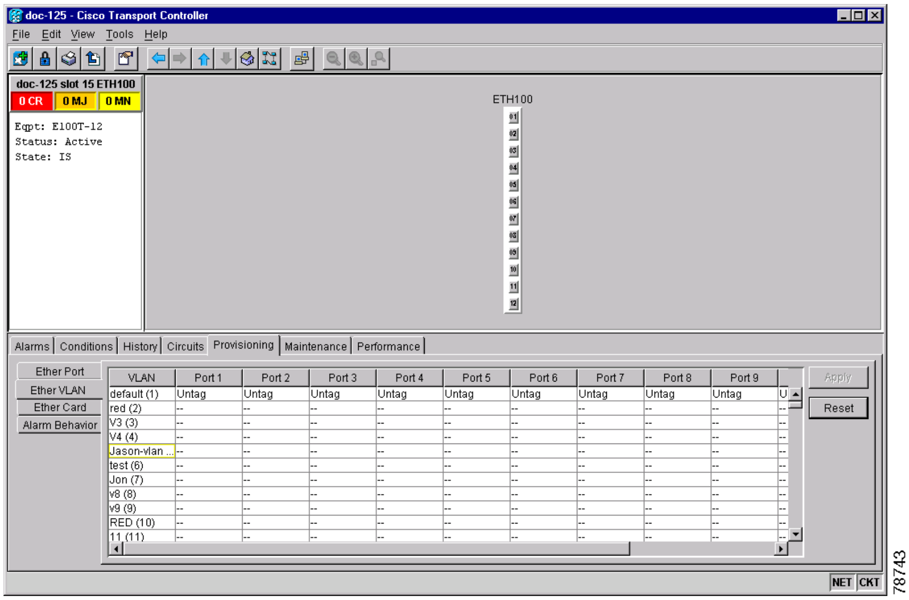
Purpose	This task provisions E series Ethernet card ports for VLAN membership
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required to enable Ethernet traffic on E series Ethernet cards
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node view.

Step 2 Double-click the E series card graphic to open the card.

Step 3 Click the **Provisioning** > **Ether VLAN** tabs (Figure 6-26).

Figure 6-26 Configuring VLAN membership for individual Ethernet ports



doc-125 - Cisco Transport Controller

doc-125 slot 15 ETH100

Eqpt: E100T-12
Status: Active
State: IS

VLAN	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	
default (1)	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag	Untag	U
red (2)	--	--	--	--	--	--	--	--	--	--
V3 (3)	--	--	--	--	--	--	--	--	--	--
V4 (4)	--	--	--	--	--	--	--	--	--	--
Jason-vlan ...	--	--	--	--	--	--	--	--	--	--
test (6)	--	--	--	--	--	--	--	--	--	--
Jon (7)	--	--	--	--	--	--	--	--	--	--
v8 (8)	--	--	--	--	--	--	--	--	--	--
v9 (9)	--	--	--	--	--	--	--	--	--	--
RED (10)	--	--	--	--	--	--	--	--	--	--
11 (11)	--	--	--	--	--	--	--	--	--	--

Step 4 To put a port in a VLAN:

a. Click the port and choose either Tagged or Untag. Figure 6-26 shows Port 1 in the red VLAN and Port 2 through Port 12 in the default VLAN. Table 6-4 shows valid port settings.

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** VLAN rows that do not need to be trunked, for example, the default VLAN.

Note Each Ethernet port must attached to at least one untagged VLAN. If a port is a trunk port, it connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (802.1Q) enabled for all the VLANs that connect to that external device.

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

Table 6-4 VLAN Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 will tag ingress frames and strip tags from egress frames.
Tagged	The ONS 15454 will process ingress frames according to the VLAN ID; egress frames will 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 individual E1000-2/E1000-2-G cards cannot be members of the same VLAN.

Step 6 Return to the circuit creation task that referred you to this task.

NTP-146 Test E Series Ethernet Circuits

Purpose	This procedure tests circuits created on E series Ethernet 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-141 Provision an E Series EtherSwitch Circuit (Multicard or Single-Card), page 6-56 NTP-142 Create an E Series Shared Packet Ring Ethernet Circuit, page 6-59 NTP-143 Create an E Series Hub and Spoke Ethernet Configuration, page 6-63
Required/As Needed	As needed
Onsite/Remote	Onsite
Security	Provisioning or higher

Step 1 Log into the ONS 15454 source Ethernet node. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 On the ONS 15454 shelf graphic, double-click the circuit source card.

Step 3 Click the **Provisioning > Ether Port** tabs.

Step 4 Verify the following settings:

- *Mode*—Is set to one of the following: 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.
- *Stp*—Checked if Spanning Tree Protocol is enabled for the circuit.

Step 5 Click the **Ether VLAN** tab.

Step 6 Verify that the source port is on the same VLAN as the destination port.

Step 7 Repeat Steps 1–6 for the destination node.

Step 8 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 will not be able to send and receive Ethernet traffic.

Step 9 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 10 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1–9 to make sure you configured the Ethernet ports and test set correctly.

Step 11 Perform protection switch testing appropriate to SONET topology:

- For UPSRs, see the "DLP-94 UPSR Protection Switching Test" task on page 5-35
- For BLSRs see the "DLP-91 BLSR Ring Switch Test" task on page 5-24.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 12 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.

NTP-147 Create a G1000-4 Ethernet Circuit

Purpose	This task creates an Ethernet circuit on the G1000-4 card.
Tools/Equipment	A G1000-4 Ethernet card must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node on the network where you will create the circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to 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 (Figure 6-27 on page 6-79), complete the following fields:

- *Name*—Assign a name to the circuit. 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.
- *Type*—Choose STS.
- *Size*—Choose the circuit size. Valid circuit sizes for a G1000-4 circuit are STS-1, STS-3c, STS6c, STS-9c, STS-12c, STS-24c, and STS-48c.
- *Bidirectional*—Leave checked for this circuit (default).
- *Number of circuits*—Leave set at 1 (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*—(default) 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-230 Change a Circuit State" task on page 9-7.

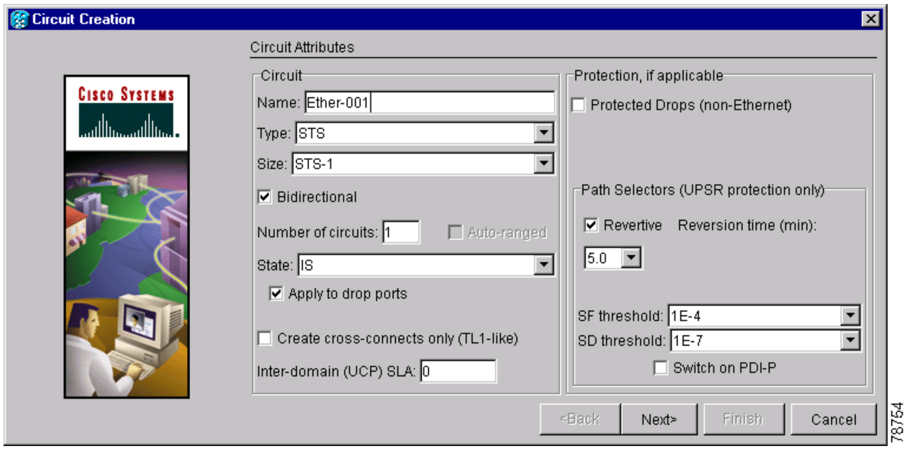
- *Apply to drop ports*—Check this box if you want to apply the state chosen in the *State* field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to G1000-4 Ethernet card ports. CTC will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms display 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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Auto-ranged*—Unavailable.
- *Protected Drops*—Leave unchecked.

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Figure 6-27 Provisioning a G1000-4 Ethernet circuit



Circuit Attributes

Circuit

Name: Ether-001

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 Click **Next**.

Step 7 Provision the circuit source:

a. From the Node pull-down menu, choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot pull-down menu, choose the slot containing the G1000-4 card that you will use for one end of the point-to-point circuit.

c. From the Port pull-down menu, choose a port.

Step 8 Click **Next**.

Step 9 Provision the circuit destination:

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

b. From the Slot pull-down menu, choose the slot containing the G1000-4 card that you will use for other end of the point-to-point circuit.

c. From the Port pull-down menu, choose a port.

Step 10 Click **Next**. The Circuits window appears.

Step 11 Confirm that the following circuit information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 circuit nodes

Step 12 Click **Finish**.

Note To change the capacity of a G1000-4 circuit, you must delete the original circuit and reprovision a new larger circuit.

Step 13 Complete the "NTP-149 Test G Series Ethernet Circuits" procedure on page 6-83.

NTP-148 Provision a G1000-4 Manual Cross-Connect

Purpose	This task manually creates a manual cross-connect between a G1000-4 Ethernet card and an OC-N cards connected to non-ONS equipment.
Tools/Equipment	A G1000-4 card must be installed at the circuit source node.
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
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 Log into a node where you will create the cross connect. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, proceed to Step 2.

Step 2 Click the **Circuits** tab and click **Create**.

Step 3 In the Create Circuits dialog box, complete the following fields:

- *Name*—Assign a name to the source cross-connect. 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 source cross-connect.
- *Type*—Choose STS.
- *Size*—Choose the size of the circuit that will be carried by the cross-connect.Valid sizes for a G1000-4 circuit are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c.

- *Bidirectional*—Leave checked for this cross-connect (default).
- *Number of circuits*—Leave set at 1 (default).
- *Auto-ranged*—Unavailable.
- *State*—Choose a service state to apply to the circuit after it is created:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—(default) 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-230 Change a Circuit State" task on page 9-7.
- *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 unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Leave unchecked.

Step 4 If the circuit will be routed on a UPSR, complete the "DLP-218 Provision UPSR Selectors During Circuit Creation" task on page 6-26.

Step 5 Click **Next**.

Step 6 Provision the circuit source:

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

b. From the Slot pull-down menu, choose the G1000-4 that will be the cross-connect source.

c. From the Port pull-down menu, choose the cross-connect source port.

Step 7 Click **Next**.

Step 8 Provision the circuit destination:

a. From the Node pull-down menu, choose the cross-connect source node selected in Step 9. (For Ethernet cross connects, the source and destination nodes are the same.)

b. From the Slot pull-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 pull-down menus.

Step 9 Click **Next**.

Step 10 Verify the cross-connection information (in this step, "circuit" refers to the cross-connect):

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 circuit nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 11 Click **Finish**.

DLP-222 Provision G1000-4 Ethernet Ports

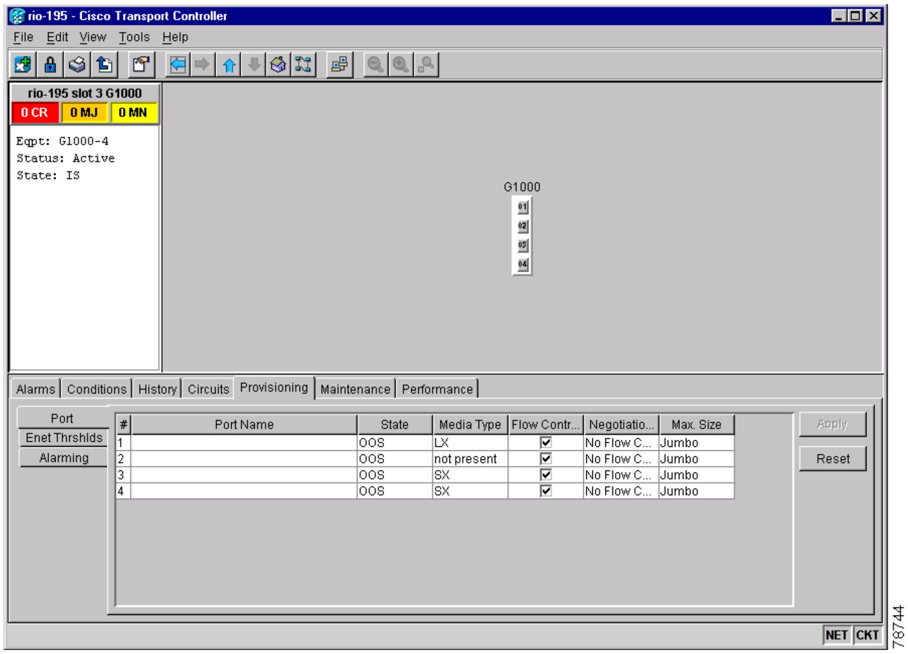
Purpose	This task provisions the G1000-4 ports for Ethernet circuits
Tools/Equipment	None
Prerequisite Procedures	NTP-127 Verify Network Turn Up, page 6-4 DLP-60 Log into CTC, page 3-22
Required/As Needed	Required to enable Ethernet traffic on the G1000-4
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node view.

Step 2 Double-click the G1000-4 card graphic to open the card.

Step 3 Click the **Provisioning** > **Port** tabs (Figure 6-28).

Figure 6-28 Provisioning G1000-4 Ethernet ports



Eqpt: G1000-4
Status: Active
State: IS

#	Port Name	State	Media Type	Flow Contr...	Negotiatio...	Max. Size
1		OOS	LX	☑	No Flow C...	Jumbo
2		OOS	not present	☑	No Flow C...	Jumbo
3		OOS	SX	☑	No Flow C...	Jumbo
4		OOS	SX	☑	No Flow C...	Jumbo

Step 4 For each G1000-4 port, provision the following parameters:

- *Port Name*—If you want to label the port, type the port name.
- *State*—Choose **IS** to put the corresponding G1000-4 Ethernet port in service.
- *Flow Control Neg*—Click this checkbox 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 G1000-4 card must be set to auto-negotiation. If flow control is enabled but the negotiation status indicates no flow control, check the auto-negotiation 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, instead of the common maximum frame size of 1518 bytes, enables the port to accept valid Ethernet frames that use protocols, such as ISL. ISL adds 30 bytes of overhead and may cause the frame size to exceed the traditional 1518 byte maximum.

Step 5 Click **Apply**.

Step 6 Refresh the Ethernet statistics:

a. Click the **Performance > Statistics** tabs.

b. Click the **Refresh** button.

Note Reprovisioning an Ethernet port on the G1000-4 card does not reset the Ethernet statistics for that port. Reprovisioning an Ethernet port on the E-series Ethernet cards resets the Ethernet statistics for that port.

Step 7 Return to your originating procedure (NTP).

NTP-149 Test G Series Ethernet Circuits

Purpose	This procedure tests circuits created on G series Ethernet 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. NTP-147 Create a G1000-4 Ethernet Circuit, page 6-78 or NTP-148 Provision a G1000-4 Manual Cross-Connect, page 6-80
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 source Ethernet node. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Change the circuit and circuit ports to out of service maintenance:

a. Click the **Circuits** tab.

b. Click the circuit you want to test.

c. From the Tools menu, choose **Circuits > Change Circuit State**.

d. On the Change Circuit State dialog box, choose **OOS_MT** from the Target Circuit State pull-down menu.

e. Check the **Apply to circuit drops** checkbox.

f. Click **OK**.

Step 3 On the ONS 15454 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—Check or unchecked as indicated by the circuit or site plan.
- Media Type—Should indicate SX, LX, or ZX.

Step 6 Repeat Steps 1–5 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 will not be 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 1–7 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform protection switch testing appropriate to SONET topology:

- For UPSRs, see the "DLP-94 UPSR Protection Switching Test" task on page 5-35.
- For BLSRs see the "DLP-91 BLSR Ring Switch Test" task on page 5-24.

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 in service:

a. Click the **Circuits** tab.

b. Choose the circuit you want to test.

c. From the Tools menu, choose **Circuits > Change Circuit State**.

d. On the Change Circuit State dialog box, choose **IS** from the Target Circuit State pull-down menu.

e. Check the **Apply to circuit drops** checkbox.

f. Click **OK**.

Step 12 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.

CHAPTER 7

Manage Alarms

This chapter explains how to view and manage the alarms and conditions on a Cisco ONS 15454.

CTC detects and reports SONET alarms generated by the Cisco ONS 15454 and the larger SONET network. You can use Cisco Transport Controller (CTC) to monitor and manage alarms at a card, node, or network level and 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-80 Document Existing Provisioning, page 7-2—Complete this procedure as needed to record node information for troubleshooting rings and spans.
2. NTP-67 View Alarms, History, Events, and Conditions, page 7-4—Complete this procedure as needed to see alarms and conditions occurring on the node and a complete history of alarm and condition messages to determine trouble occurrence patterns when troubleshooting.
3. NTP-68 Delete Cleared Alarms from Display, page 7-12—Complete this procedure as needed to delete cleared alarm information that is no longer needed.
4. NTP-69 View Alarm-Affected Circuits, page 7-13—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. NTP-70 View Alarm Counts on the LCD for a Slot or Port, page 7-15—Complete this procedure as needed to see a statistical count of alarms that have occurred for a slot or port.
6. NTP-71 Create, Download, and Assign Alarm Severity Profiles, page 7-16—Complete this procedure as needed to change the default severity for certain alarms, assign the new severities to a port, card, or node, and delete alarm profiles.
7. NTP-168 Enable, Modify, or Disable Alarm Severity Filtering, page 7-30—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens; you can enable, modify, and disable alarm severity filtering at the node or network level.
8. NTP-72 Suppress and Unsuppress Alarm Reporting, page 7-37—As needed, use these tasks to suppress reported alarms at the port, card, or node level and disable the suppress command to resume normal alarm reporting.

NTP-80 Document Existing Provisioning

Purpose	Use this procedure to record node information for troubleshooting rings and spans.
Tools/Equipment	A printer must be connected to the CTC computer
Prerequisite Procedures	Chapter 4, "Turn Up Node"
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 that has the information you want to record or save. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 If you need to document information that you cannot write down, or need to preserve, you can do so by

- Copying and pasting CTC text into other applications using the Windows Copy (Ctrl+C), Cut (Ctrl+X), and Paste (Ctrl+V) commands.
- Printing information with the "DLP-138 Print CTC Data" task on page 7-2.
- Saving information to a word processing application such as a spreadsheet; complete the "DLP-139 Export CTC Data" task on page 7-3.

DLP-138 Print CTC Data

Purpose	Use this task to print CTC windows and CTC table data such as alarms and inventory.
Tools/Equipment	A printer must be connected to the CTC computer
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

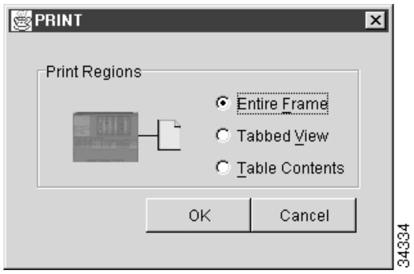
Step 1 Click the CTC tab containing the information you want to print (for example, the Alarms tab or the Circuits tab).

Step 2 From the CTC File menu, click **Print**.

Step 3 In the Print dialog box choose an option (Figure 7-1):

- *Entire Frame*—Prints the entire CTC window
- *Tabbed View*—Prints the lower half of the CTC window
- *Table Contents*—Prints CTC data in table format; this option is only available for CTC table data (see the "Table Display Options" section on page A-7).

Figure 7-1 Selecting CTC data for print



Print Regions

● Entire Frame
○ Tabbed View
○ Table Contents

Step 4 Click **OK**.

Step 5 In the Windows Print dialog box, choose a printer and click **Print**.

Step 6 Repeat this task for each tab that you want to print.

Step 7 Return to your originating procedure (NTP).

DLP-139 Export CTC Data

Purpose	Use this task to export CTC table data for use by other applications such as spreadsheets, word processors, and database management applications.
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

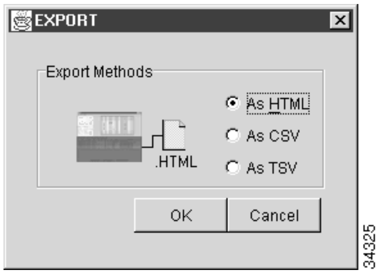
Step 1 Click the CTC tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).

Step 2 From the CTC File menu, click **Export**.

Step 3 In the Export dialog box (Figure 7-2) choose a format for the data:

- *As HTML*—Saves the data as an HTML file. The file can be viewed with a web browser (such as Netscape Navigator or Microsoft Internet Explorer) without running CTC. Use the browser's File/Open command to open the CTC data file.
- *As CSV*—Saves the CTC table values as text, separated by commas. You can import CSV data into spreadsheets and database management programs.
- *As TSV*—Saves the CTC table values as text, separated by tabs. You can import TSV data into spreadsheets and database management programs.

Figure 7-2 Selecting CTC data for export



● As HTML

Step 4 Click **OK**.

Step 5 In the Save dialog box, enter a file name in one of the following formats:

- *[filename].htm*—for HTML files
- *[filename].csv*—for CSV files
- *[filename].tsv*—for TSV files

Step 6 Navigate to a directory where you want to store the file.

Step 7 Click **OK**.

Step 8 Repeat the task for each tab that you want to export.

Note CTC data exported as comma separated values (CSV) or tab separated values (TSV) can be viewed in text editors, word processors, spreadsheets, and database management applications. Although procedures depend on the application, you typically can use File/Open to display the CTC data. Text editors and word processors display the data exactly as it is exported. Spreadsheet and database management applications display the data in cells. You can then format and manage the data using the spreadsheet or database management application tools.

Step 9 Return to your originating procedure (NTP).

NTP-67 View Alarms, History, Events, and Conditions

Purpose	Use this procedure to view alarms and conditions occurring on the node and to retrieve a complete history of event messages.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

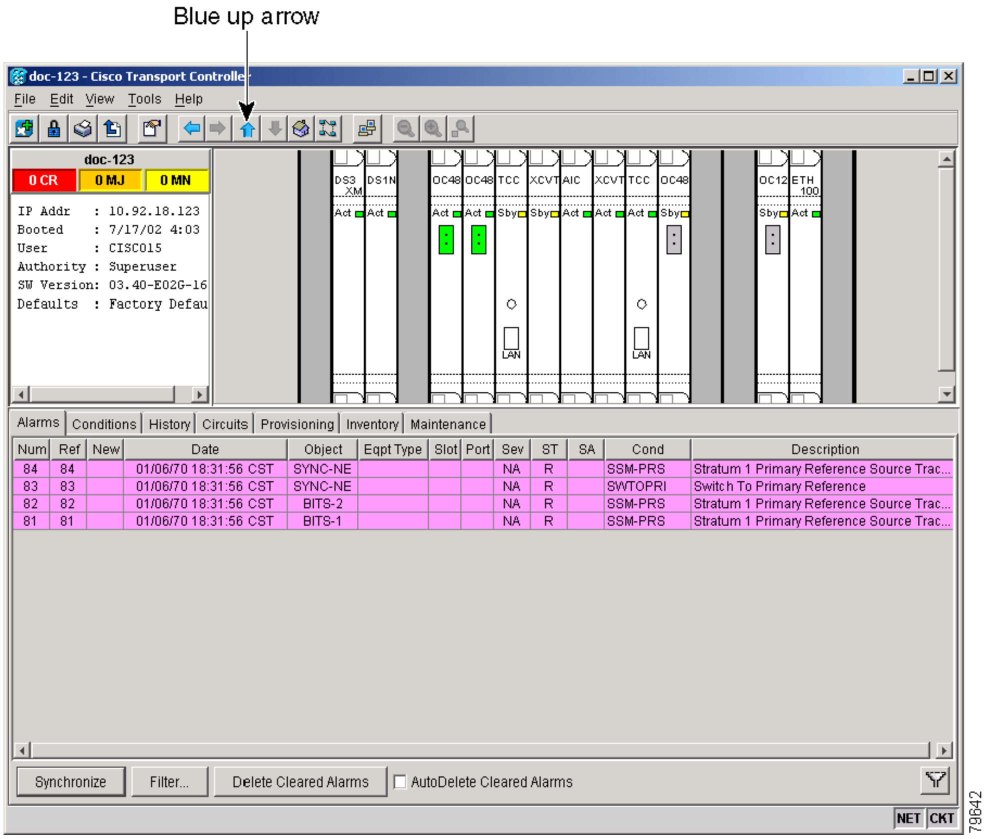
Step 1 Log into the node that contains the alarms you want to view. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 At the card, node, or network-level CTC view, click the **Alarms** tab to display the alarms for that card, node, or network (Figure 7-3).

Step 3 Troubleshoot the alarms using the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Complete the "DLP-110 View Alarm History" task on page 7-6, the "DLP-113 View Events and Synchronize Alarms" task on page 7-9, or the "DLP-114 View Conditions" task on page 7-10 as needed.

Figure 7-3 Viewing alarms in the CTC network view


Blue up arrow

```
IP Addr   : 10.92.18.123
Booted    : 7/17/02 4:03
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
84	84		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
83	83		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
82	82		01/06/70 18:31:56 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
81	81		01/06/70 18:31:56 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

DLP-110 View Alarm History

Purpose	Use this task to view past cleared and uncleared ONS 15454 alarm messages at the card, node, or network level.
Tools/Equipment	None
Prerequisite Procedures	None
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.

For the node-level alarm history, go to Step 2. For the network-level alarm message history, go to Step 3. For the card-level alarm message history, go to Step 5.

Step 2 The node-level view is the default view after you log into CTC (Figure 7-4 on page 7-7). To display the node-level alarm message history:

a. Click the **History > Session** tabs if you want to see only the alarm messages and event messages that have occurred since you logged into the CTC.

b. Click the **History > Node** tabs if you want to retrieve all available alarm messages for the node. Go to Step 6.

Step 3 From the node (default login) view (Figure 7-4 on page 7-7), display the network view.

Step 4 Click the **History** tab. Alarm messages and event messages that have occurred on the network since you logged into CTC are displayed. Go to Step 9.

Step 5 Double-click a card on the shelf graphic of any card besides the TCC+ or cross-connect card to display the card-level view for the card.

a. Click the **History > Session** tabs if you want to see only the alarm messages and event messages that have occurred since you logged into CTC.

b. Click the **History > Card** tabs if you want to retrieve all available alarm messages for the card. Go to Step 6.

Note The ONS 15454 can store up to 640 critical alarm raise/clear messages, 640 major alarm raise/clear messages, 640 minor alarm raise/clear messages, and 640 event-level raise/clear/transient messages. When any of these limits is reached, the ONS 15454 discards the oldest alarms and events in that category.

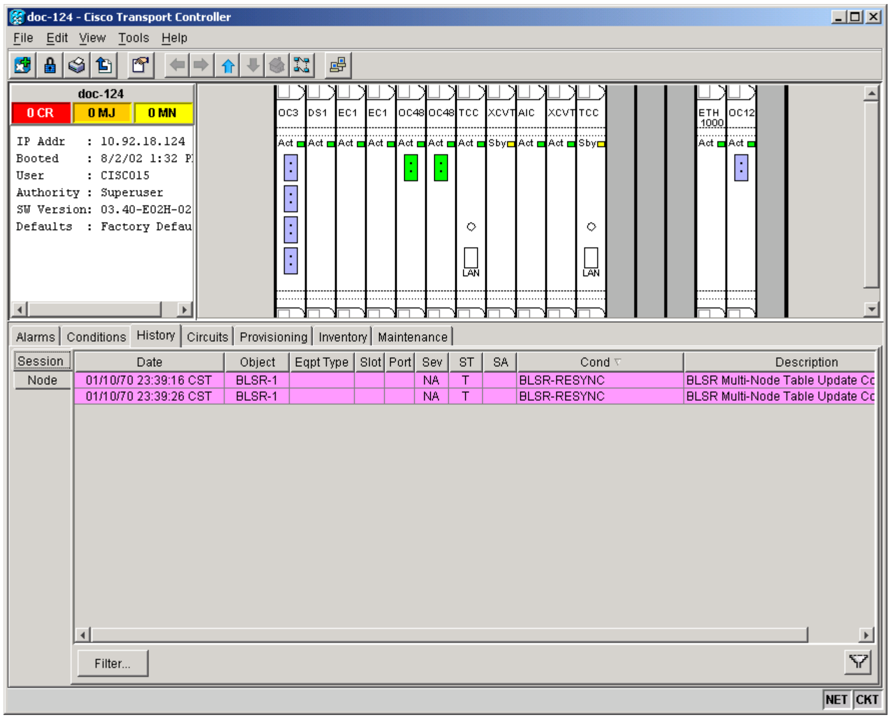
Step 6 Verify that the **Alarms** checkbox is selected in the History > Node tabs and/or History > Card tabs to ensure that alarm messages and event messages with a severity of minor (MN), major (MJ), or critical (CR) – are reported.

Step 7 If you want to retrieve event messages, click the **Events** checkbox in the History > Node and/or History > Card tabs. Event messages include transient messages and also raise/clear messages for Not Alarmed (NA) standing conditions.

Step 8 In the History > Node and/or History > Card tabs, click the **Retrieve** button. Alarm messages are automatically shown in the network view.

Tip Double-click an alarm in the alarm table or an event 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 (default login) view.

Figure 7-4 Viewing alarm history for the current session



```
IP Addr  : 10.92.18.124
Booted   : 8/2/02 1:32 P
User     : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02
Defaults  : Factory Defau
```

Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
01/10/70 23:39:16 CST	BLSR-1				NA	T		BLSR-RESYNC	BLSR Multi-Node Table Update Cc
01/10/70 23:39:26 CST	BLSR-1				NA	T		BLSR-RESYNC	BLSR Multi-Node Table Update Cc

Step 9 Return to your originating procedure (NTP).

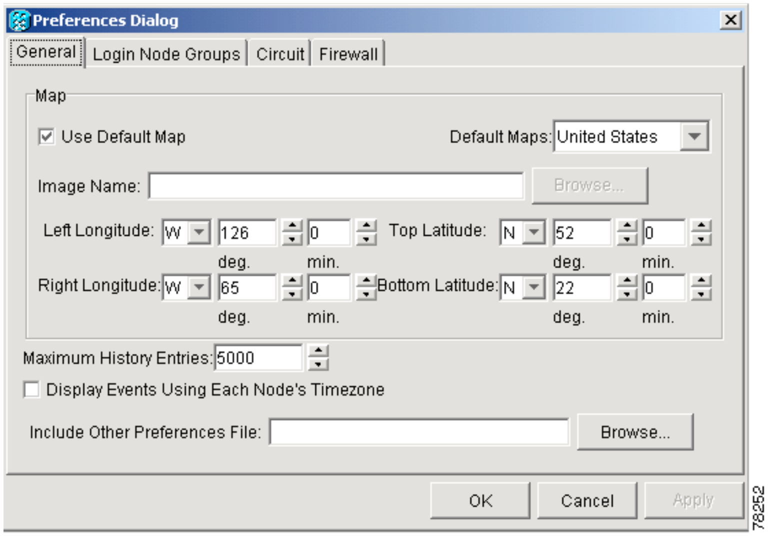
DLP-111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	Use this task to change the maximum number of session entries displayed by the alarm history from the default of 5000.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 At the card, node, or network view, from the CTC menu bar click **Edit > Preferences**.

The CTC Preferences Dialog appears (Figure 7-5).

Figure 7-5 CTC Preferences Dialog featuring Maximum History Entries



☑ Use Default Map

Default Maps: United States

Image Name:

Left Longitude: W 126 deg. 0 min.

Top Latitude: N 52 deg. 0 min.

Right Longitude: W 65 deg. 0 min.

Bottom Latitude: N 22 deg. 0 min.

Maximum History Entries: 5000

□ Display Events Using Each Node's Timezone

Include Other Preferences File:

Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry to the desired number. The permitted range of maximum history entries is from 500 to 100,000. When the value is changed, the Apply button is enabled.

Step 3 Click **Apply** and **OK**.

Note Setting the maximum history entries entry 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).

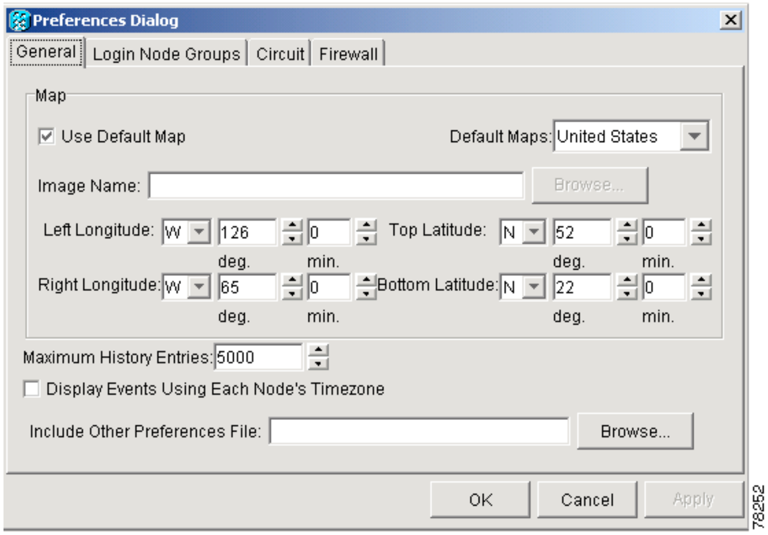
DLP-112 Display Alarms and Events Using Each Node's Timezone

Purpose	Use this task to change 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-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 At the card, node, or network view, from the CTC menu bar click **Edit > Preferences**.

The CTC Preferences Dialog appears (Figure 7-6).

Figure 7-6 CTC Preferences Dialog featuring Maximum History Entries



☑ Use Default Map
Default Maps: United States
Image Name:
Left Longitude: W 126 deg. 0 min.
Top Latitude: N 52 deg. 0 min.
Right Longitude: W 65 deg. 0 min.
Bottom Latitude: N 22 deg. 0 min.
Maximum History Entries: 5000
☐ Display Events Using Each Node's Timezone
Include Other Preferences File:

Step 2 Click the **Display Events Using Each Node's Timezone** checkbox. The Apply button is enabled.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-113 View Events and Synchronize Alarms

Purpose	Use this task to view ONS 15454 events at the card, node, or network level and synchronize the alarm listing while troubleshooting to check for cleared alarms or conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 the **Synchronize** button.

This button causes CTC to retrieve a current alarm summary for the node. This step is optional, since CTC updates the Alarms tab automatically as raise/clear messages arrive from the node.

Step 3 Return to your originating procedure (NTP).

DLP-114 View Conditions

Purpose	Use this task to view conditions at the card, node, or network level.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 the **Retrieve** button (Figure 7-7 on page 7-11).

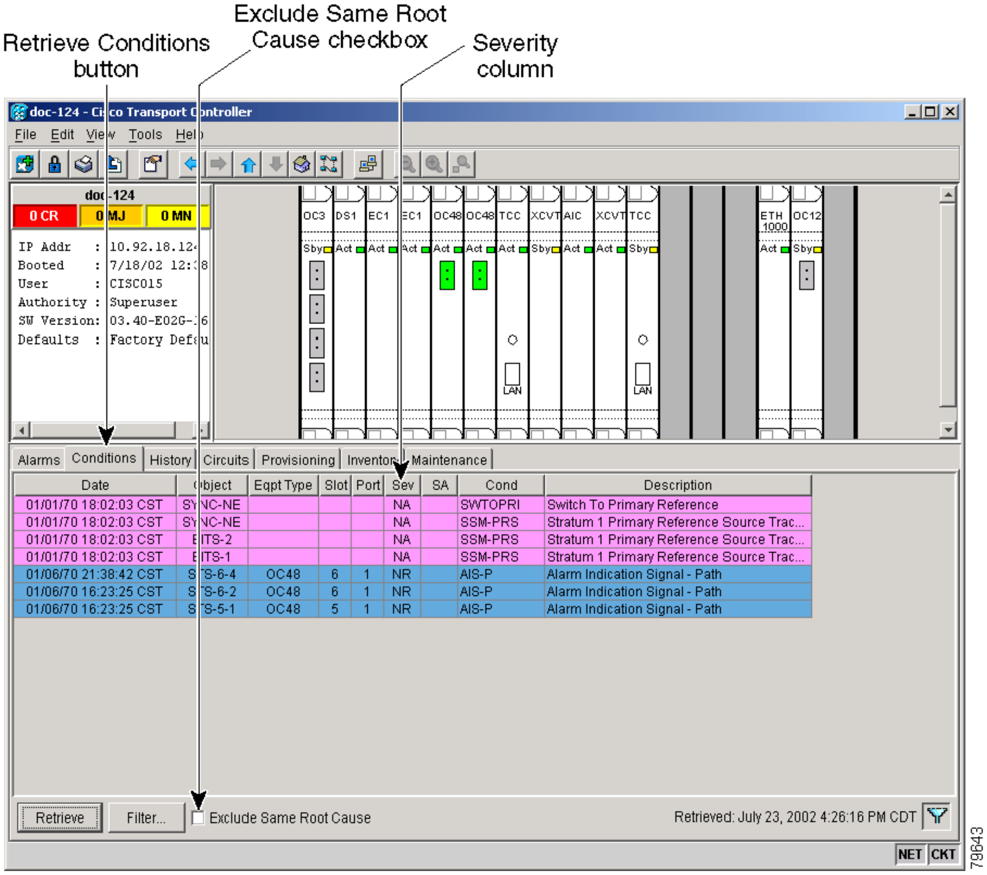
Conditions include all fault conditions raised on the node, whether or not they are reported (i.e. messages sent) to CTC and other clients. Conditions that are reported at Major, Minor, or Critical severities are alarms. Conditions that are reported at Not Alarmed are events. Conditions that are not reported at all are marked as Not Reported in the Conditions tab severity column.

Clicking Retrieve requests the current set of fault conditions from the node. The tab is not updated when things change on the node. The operator must click Retrieve to see any changes.

Conditions have a default severity of CR, MJ, MN, or NA but are not reported at this time due to exclusion or suppression (by CTC command or port or circuit state other than IS) are shown as NR on the Conditions tab. Conditions that are currently reported are shown at the chosen reporting severity.

Note When ONS 15454 ports are placed in the out-of-service (OOS) state, OOS maintenance (OOS-MT) state, or OOS auto-in-service (OOS-AINS) state for loopback testing operations, traffic passes and performance-monitoring information is collected, but alarming is suppressed. The alarms are not reported autonomously, but can be retrieved.
When ports are placed in OOS state, the Alarms Suppressed for Maintenance (AS-MT) condition is raised on them. For more information about placing the ONS 15454 in OOS state for performing loopback tests, or for information about alarm troubleshooting, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Figure 7-7 Viewing fault conditions retrieved under the Conditions tabs



```
IP Addr   : 10.92.18.124
Booted    : 7/18/02 12:38
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Date	Object	Eqpt Type	Slot	Port	Sev	SA	Cond	Description
01/01/70 18:02:03 CST	SYNC-NE				NA		SWTOPRI	Switch To Primary Reference
01/01/70 18:02:03 CST	SYNC-NE				NA		SSM-PRS	Stratum 1 Primary Reference Source Trac...
01/01/70 18:02:03 CST	BITS-2				NA		SSM-PRS	Stratum 1 Primary Reference Source Trac...
01/01/70 18:02:03 CST	BITS-1				NA		SSM-PRS	Stratum 1 Primary Reference Source Trac...
01/06/70 21:38:42 CST	STS-6-4	OC48	6	1	NR		AIS-P	Alarm Indication Signal - Path
01/06/70 16:23:25 CST	STS-6-2	OC48	6	1	NR		AIS-P	Alarm Indication Signal - Path
01/06/70 16:23:25 CST	STS-5-1	OC48	5	1	NR		AIS-P	Alarm Indication Signal - Path

□ Exclude Same Root Cause

Retrieved: July 23, 2002 4:26:16 PM CDT

Step 3 If you want to apply exclusion rules, click the **Exclude Same Root Cause** checkbox at the node or network view.

According to Telcordia, exclusion rules apply to a query of “all conditions from a node” (the rules that apply in a "RTRV-ALM-ALL" TL1 command, but not in more specific TL1 RTRV-ALM commands). To match TL1 retrieval results, click the **Exclude Same Root Cause** checkbox on node view and network view, and leave it unchecked on card view.

Step 4 Return to your originating procedure (NTP).

NTP-68 Delete Cleared Alarms from Display

Purpose	Use this procedure to delete cleared alarms and transient messages from the CTC display when they are not needed for long-term information or later troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Log into a node where you want to delete alarms. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

To delete node-level alarms, go to Step 2. To delete card-level alarms, go to Step 3. To delete network-level alarms, go to Step 4.

Step 2 To delete node-level alarms:

a. On the node (default) view click the **Alarms** tab.

b. Click **Delete Cleared Alarms**, referring to the rules in c..

This action will remove any cleared ONS 15454 alarms from the Alarms display. The rows of cleared alarms are colored white and have a C in their status (ST) column (Figure 7-7 on page 7-12).

Step 3 To delete card-level alarms:

a. On the node (default login) view, double-click the card graphic for the card you want to open.

b. Click the **Alarms** tab and then click the **Delete Cleared Alarms** button, referring to the rules in Step 5.

Step 4 To delete network-level alarms:

a. On the node (default login) view, click the blue up arrow tool on the toolbar at the top of the CTC window to display the network view.

b. Click the **Alarms** tab and then click the **Delete Cleared Alarms** button, referring to the rules in Step 5.

Step 5 Consult the following rules when deleting cleared alarms from the display:

a. If the **Autodelete Cleared Alarms** checkbox is checked, an alarm will disappear from the tab when it is cleared.

b. If the **Autodelete Cleared Alarms** checkbox is not checked, an alarm will remain on the tab when it is cleared as an item that displays white on the tab with the severity Clear (CL). The item can be removed by clicking Delete Cleared Alarms.

c. Transient messages are single message, not raise/clear pairs (i.e. they do not have a companion message). Click **Delete Cleared Alarms** to remove the transients from the tab.

NTP-69 View Alarm-Affected Circuits

Purpose	Use this procedure to view all circuits affected by a past or present alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Log into the ONS 15454. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

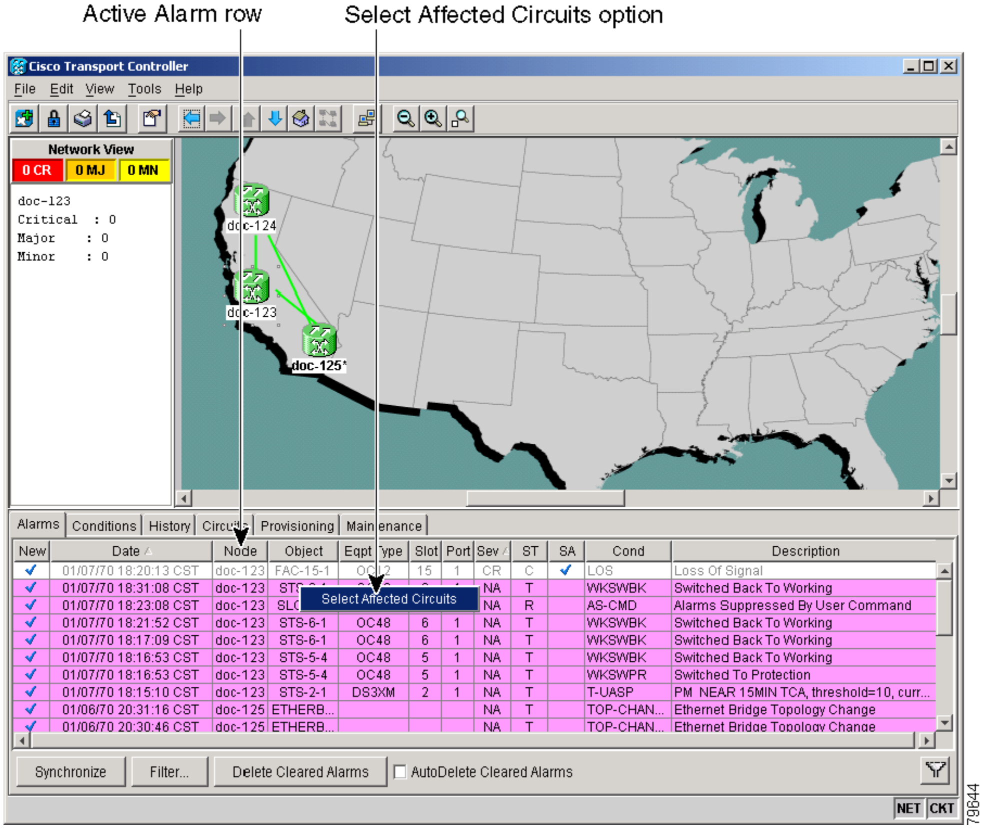
Step 2 In the network, node, or card view, click the **Alarms** tab and then right-click anywhere on the row of an active alarm.

Note The node view is the default, but you can also navigate to the Alarms tab in the network view and card view to perform Step 2.

Note The card view is not available for the TCC+ or cross-connect cards.

The Select Affected Circuit option appears on the shortcut menu (Figure 7-8 on page 7-14).

Figure 7-8 Selecting the Affected Circuits option



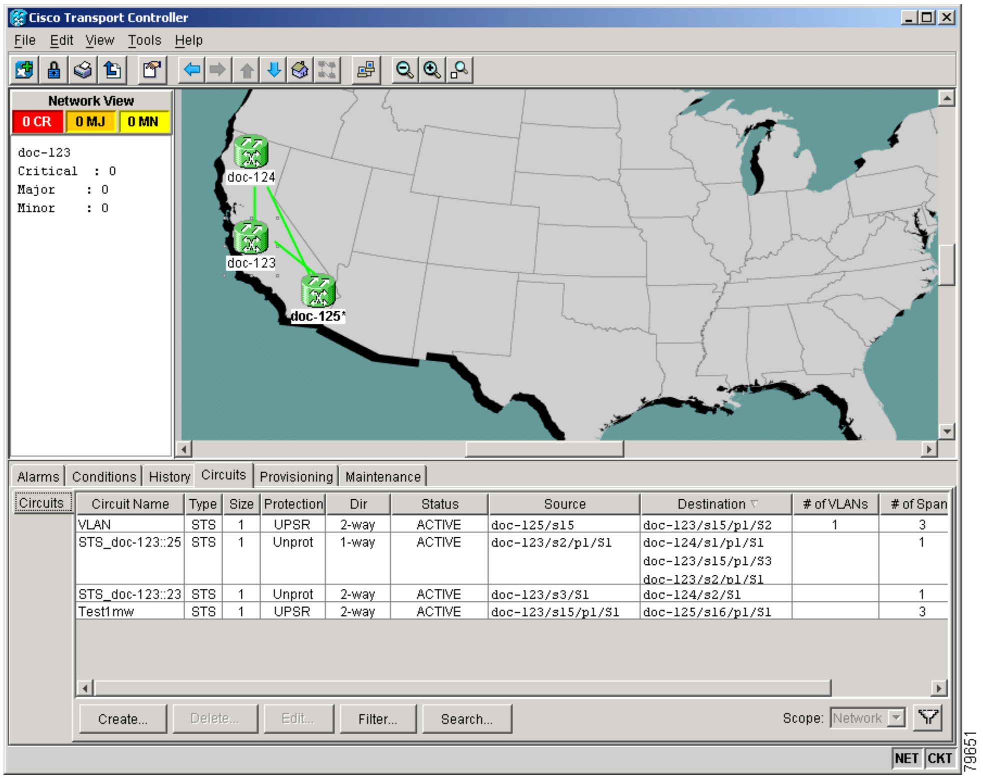
doc-123
Critical : 0
Major : 0
Minor : 0

New	Date	Node	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
✓	01/07/70 18:20:13 CST	doc-123	FAC-15-1	OC12	15	1	CR	C	✓	LOS	Loss Of Signal
✓	01/07/70 18:31:08 CST	doc-123	STS				NA	T		WKSWBK	Switched Back To Working
✓	01/07/70 18:23:08 CST	doc-123	SLC				NA	R		AS-CMD	Alarms Suppressed By User Command
✓	01/07/70 18:21:52 CST	doc-123	STS-6-1	OC48	6	1	NA	T		WKSWBK	Switched Back To Working
✓	01/07/70 18:17:09 CST	doc-123	STS-6-1	OC48	6	1	NA	T		WKSWBK	Switched Back To Working
✓	01/07/70 18:16:53 CST	doc-123	STS-5-4	OC48	5	1	NA	T		WKSWBK	Switched Back To Working
✓	01/07/70 18:16:53 CST	doc-123	STS-5-4	OC48	5	1	NA	T		WKSWPR	Switched To Protection
✓	01/07/70 18:15:10 CST	doc-123	STS-2-1	DS3XM	2	1	NA	T		T-UASP	PM NEAR 15MIN TCA, threshold=10, curr...
✓	01/06/70 20:31:16 CST	doc-125	ETHERB...				NA	T		TOP-CHAN...	Ethernet Bridge Topology Change
✓	01/06/70 20:30:46 CST	doc-125	ETHERB...				NA	T		TOP-CHAN...	Ethernet Bridge Topology Change

Step 3 Left-click or right-click **Select Affected Circuits**.

The **Circuits** pane appears with affected circuits highlighted (Figure 7-9 on page 7-15).

Figure 7-9 Highlighted circuit appears



doc-123
Critical : 0
Major : 0
Minor : 0

Circuit Name	Type	Size	Protection	Dir	Status	Source	Destination	# of VLANs	# of Span
VLAN	STS	1	UPSR	2-way	ACTIVE	doc-125/s15	doc-123/s15/p1/S2	1	3
STS_doc-123::25	STS	1	Unprot	1-way	ACTIVE	doc-123/s2/p1/S1	doc-124/s1/p1/S1 doc-123/s15/p1/S3 doc-123/s2/p1/S1		1
STS_doc-123::23	STS	1	Unprot	2-way	ACTIVE	doc-123/s3/S1	doc-124/s2/S1		1
Test1mw	STS	1	UPSR	2-way	ACTIVE	doc-123/s15/p1/S1	doc-125/s16/p1/S1		3

Step 4 If you want to search for particular circuits, refer to the "DLP-131 Search for Circuits" procedure on page 9-5.

NTP-70 View Alarm Counts on the LCD for a Slot or Port

Purpose	Use this procedure to view a statistical count of alarms that have occurred for a slot or port to help in problem identification or elimination.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Press the **Slot** button on the LCD panel to toggle to the desired slot number on the ONS 15454.

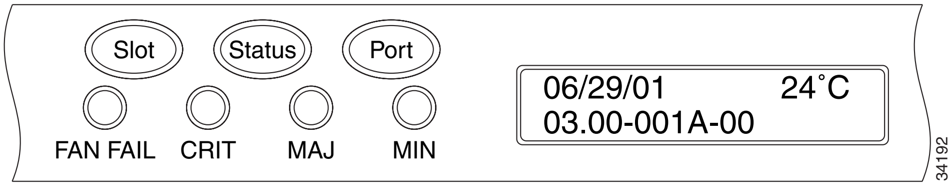
Step 2 If you want a card-level alarm count, press the **Status** button.

Step 3 Press the **Port** button to toggle to a specific port.

Step 4 If you want a port-level alarm count, press the **Status** button on the LCD panel.

Figure 7-10 shows the LCD panel.

Figure 7-10 The LCD panel



Note A blank LCD results when the fuse on the AIP board is blown. If this occurs, call Cisco TAC at 1-877-323-7368.

Note Use the Slot button to toggle to Node to see a summary of alarms for the entire node.

NTP-71 Create, Download, and Assign Alarm Severity Profiles

Purpose	Use this procedure to change the default severity for certain alarms; assign the new severities to a port, card, or node; and delete 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 Log into a node where you want to create an alarm profile. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2. Go to Step 2 to clone or modify an alarm profile, or Step 3 to download an alarm profile.

Step 2 Complete the "DLP-115 Create Alarm Severity Profiles" task on page 7-17. This task clones a current alarm profile, renames the profile, and customizes the new profile. Go to Step 4.

Step 3 Complete the "DLP-223 Download an Alarm Severity Profile" procedure on page 7-20. This task downloads an alarm severity profile from a CD or a node.

Step 4 As necessary, complete the "DLP-116 Apply Alarm Profiles to Ports" task on page 7-24 or the "DLP-117 Apply Alarm Profiles to Cards and Nodes" task on page 7-26.

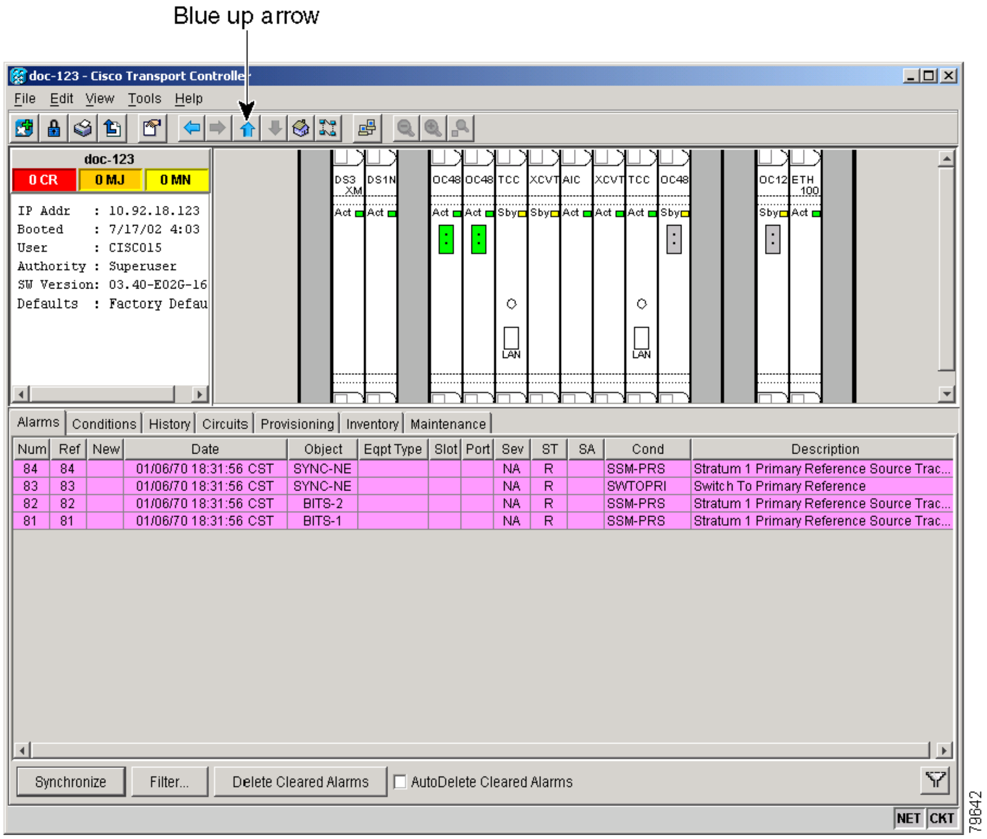
DLP-115 Create Alarm Severity Profiles

Purpose	Use this task to create custom severity profiles for alarms that differ from the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the node (default login) view, click the blue up arrow tool to display the network view.

Figure 7-11 shows the blue up arrow tool on the node (default login) view.

Figure 7-11 Blue up arrow tool on node (default login) view



```
IP Addr    : 10.92.18.123
Booted     : 7/17/02 4:03
User       : CISCO15
Authority  : Superuser
SW Version: 03.40-E02G-16
Defaults   : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
84	84		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
83	83		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
82	82		01/06/70 18:31:56 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
81	81		01/06/70 18:31:56 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

☐ AutoDelete Cleared Alarms

Step 2 Click the **Provisioning > Alarm Profiles** tabs (Figure 7-12 on page 7-18).

Step 3 Click the **Load** button.

Step 4 In the Select Profile(s) or Filename to Load window, click the **From Node** radio button.

Step 5 Highlight the node name you are logged into in the Node Names list.

Step 6 Highlight **Default** in the Profile Names list.

Step 7 Click **OK**.

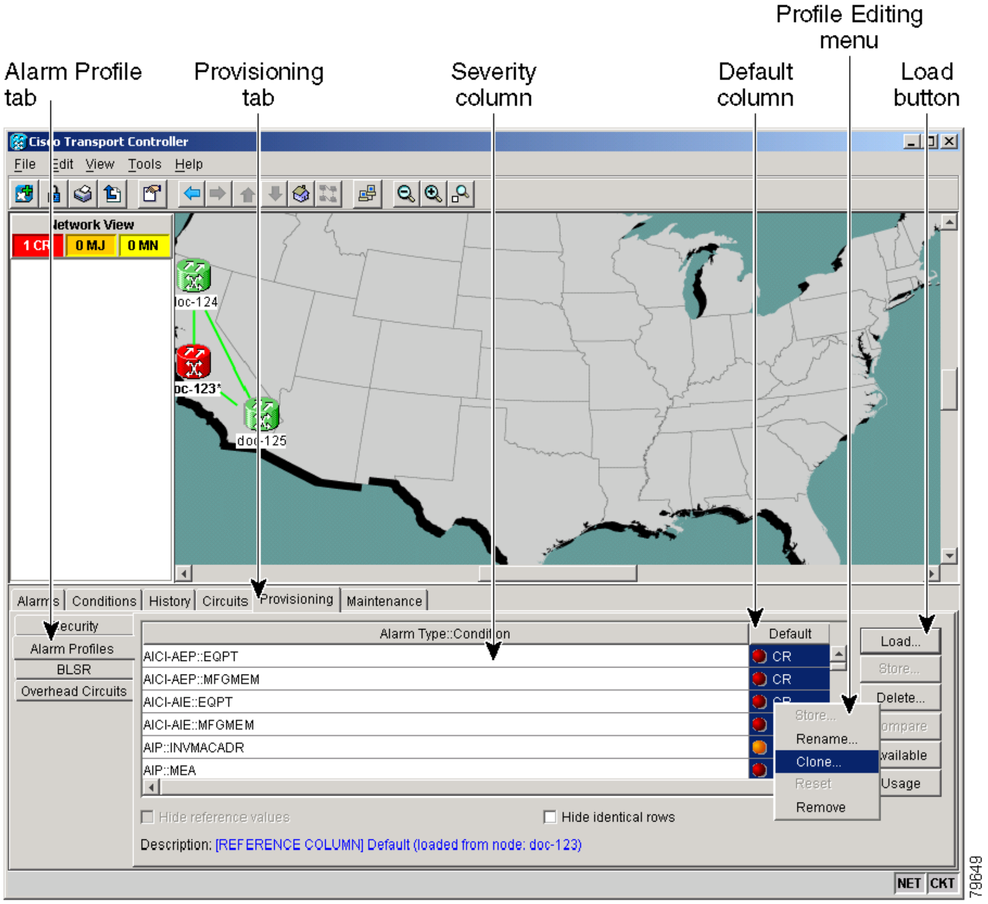
The Default alarm severity profile appears in the Alarm Profiles tab pane.

Step 8 Right-click anywhere in the Default profile column to display the profile editing shortcut menu.

Step 9 Choose **Clone** from the menu.

You can also clone any other profiles that appear under the Available button, except Inherited.

Figure 7-12 Alarm profiles window showing the default profiles of the listed alarms



Alarm Type::Condition	Default
AICI-AEP::EQPT	CR
AICI-AEP::MFGMEM	CR
AICI-AIE::EQPT	CR
AICI-AIE::MFGMEM	
AIP::INVMACADR	
AIP::MEA	

□ Hide reference values □ Hide identical rows

Description: [REFERENCE COLUMN] Default (loaded from node: doc-123)

Step 10 In the 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.

Tip You can also clone alarm profiles shown when you click the Available button in the Provisioning > Alarm Profiles tabs.

Step 11 Click **OK**.

A new alarm profile (named in Step 10) is created. This profile duplicates the severities of the default profile and is added as a new column on the right side of the Alarm Profiles tab.

Step 12 Modify (customize) the alarm profile:

a. In the new alarm profile column, left-click in a row that contains the alarm severity you want to change.

b. From the pull-down menu, choose the desired severity.

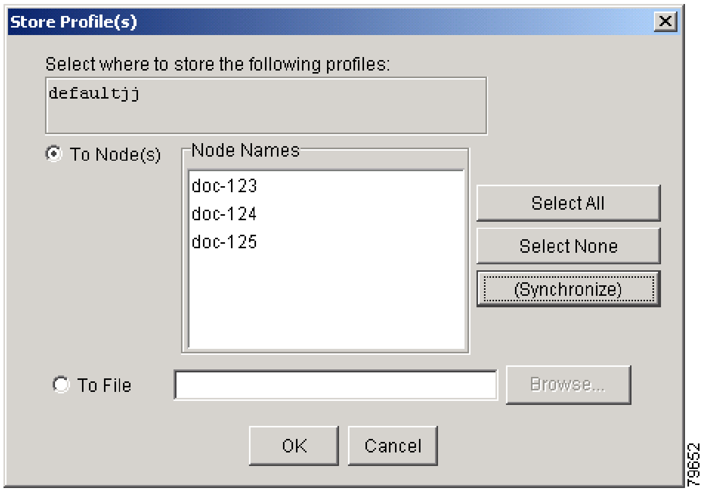
c. Repeat Steps a and b for each alarm that needs to be changed.

Step 13 After you have assigned the properties to the new alarm profile, right-click anywhere in the column of the new alarm profile to highlight it.

Step 14 On the profile editing shortcut menu, choose **Store**.

Step 15 In the Store Profile(s) dialog box, click the *To Node(s)* radio button or the *To File* radio button (Figure 7-13).

Figure 7-13 Store Profile(s) dialog window



Store Profile(s)

Select where to store the following profiles:

defaulttjj

● To Node(s)

Node Names

doc-123
doc-124
doc-125

Step 16 If you selected To Node(s), go to Step a. If you selected To File, go to Step b.

a. Choose the login node from the **Node Names** list, and click one of the following buttons:

- *Select All*—Selects all node names in the Node Names list. (This will also select all nodes if none are highlighted in the list.)
- *Select None*—Selects none of the node names in the Node Names list. (This will also select none of the nodes in the list even if they have been highlighted.)
- *(Synchronize)*—Updates the alarm profile information.

Go to Step c.

b. Click the **Browse** button to choose a file destination on the workstation.

c. Enter a filename in the name field.

Long file names are supported. CTC supplies a suffix of *.pfl.

d. Click **OK**.

Step 17 Return to your originating procedure (NTP).

Note Checking the **Hide identical rows** checkbox configures the Alarm Profiles tab pane to display only the rows of the profile severities that do not match, along with the row's specific alarm type and condition.

Note Checking the **Hide values matching profile Default** checkbox configures the Alarm Profiles tab pane to display only the severities that do not match the severities of the Default profile.

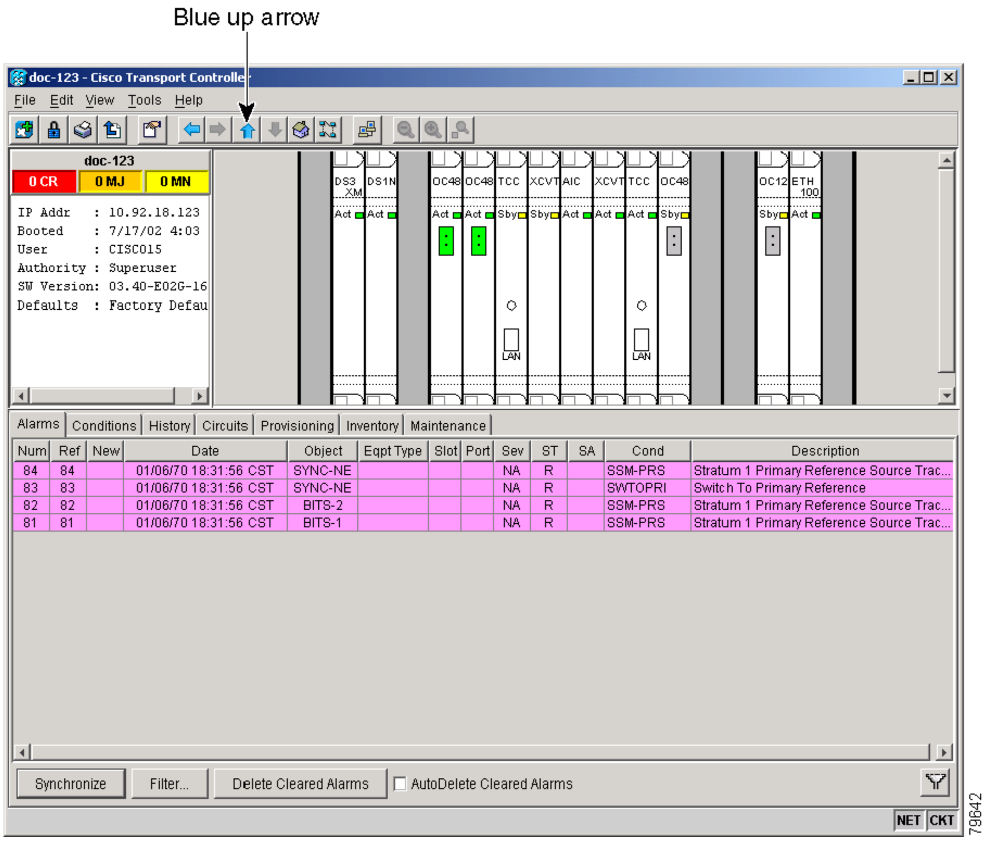
DLP-223 Download an Alarm Severity Profile

Purpose	Use this task to download a custom alarm severity profile from a CD or another node.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the node (default login) view, click the blue up arrow tool to display the network view.

Figure 7-14 on page 7-21 shows the blue up arrow tool on the node (default login) view.

Figure 7-14 Blue up arrow tool on node (default login) view



Blue up arrow

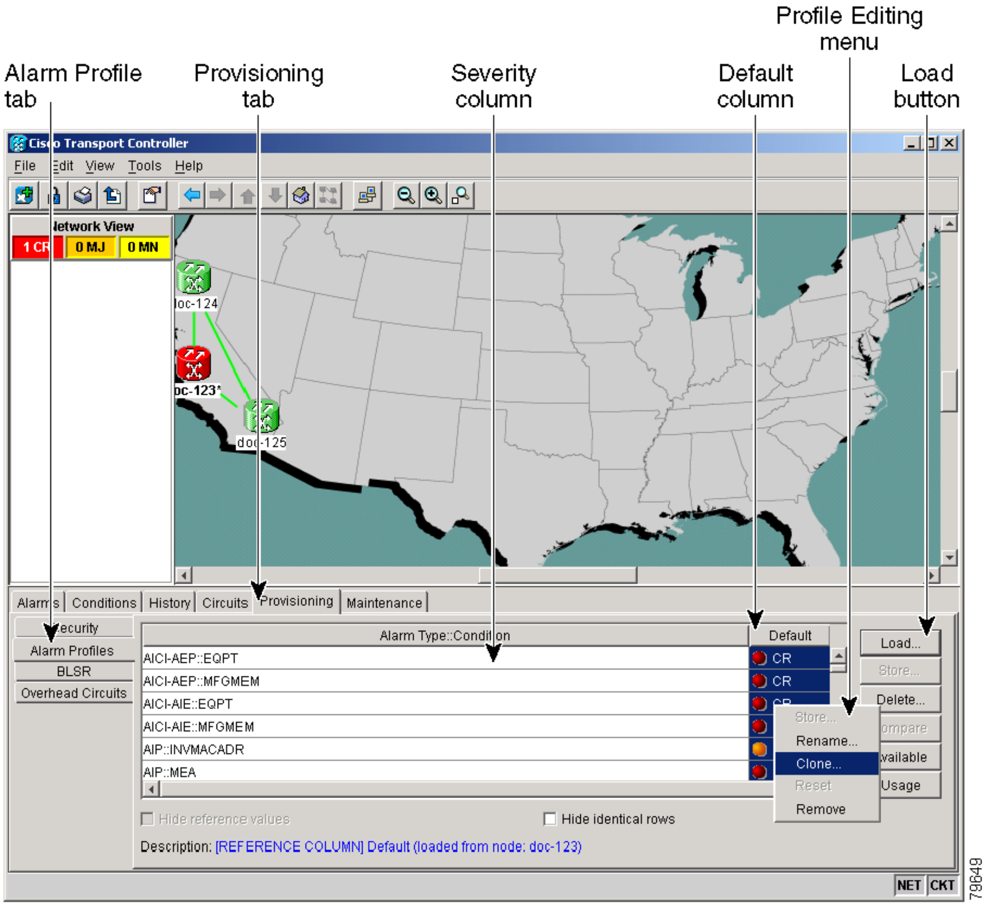
```
IP Addr   : 10.92.18.123
Booted    : 7/17/02 4:03
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
84	84		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
83	83		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
82	82		01/06/70 18:31:56 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
81	81		01/06/70 18:31:56 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

☐ AutoDelete Cleared Alarms

Step 2 Click the **Provisioning > Alarm Profiles** tabs (Figure 7-15 on page 7-22).

Figure 7-15 Alarm window showing the default profiles of the listed alarms



Alarm Type::Condition	Default
AICI-AEP::EQPT	CR
AICI-AEP::MFGMEM	CR
AICI-AIE::EQPT	CR
AICI-AIE::MFGMEM	
AIP::INVMACADR	
AIP::MEA	

□ Hide reference values □ Hide identical rows

Description: [REFERENCE COLUMN] Default (loaded from node: doc-123)

Step 3 Click **Load**.

If you want to download a file from the local PC, a CD, or a network drive (if connected), go to Step 4. If you want to download a file from another connected node, go to Step 5.

Step 4 In the Select Profile(s) from Node or Filename to Load window, click the **From File** radio button.

a. Click the **Browse** button.

The Open dialog box appears.

b. In the Look in pull-down menu, navigate to the folder on the local PC hard drive, CD, or network (if connected) where the profile file is located.

c. Click the name in the window to highlight it.

The file must have the *.pfl extension.

d. Click the **Open** button.

e. Go to Step 6.

Step 5 In the Select Profile(s) from Node or Filename to Load window, click the **From Node** radio button if it is not already selected.

a. Under the Node Names list, click the node you want to download the existing profile from.

b. Under the Profile Names list, click the profile you want to download.

Step 6 In the Select Profile(s) from Node or Filename to Load window, click **OK**.

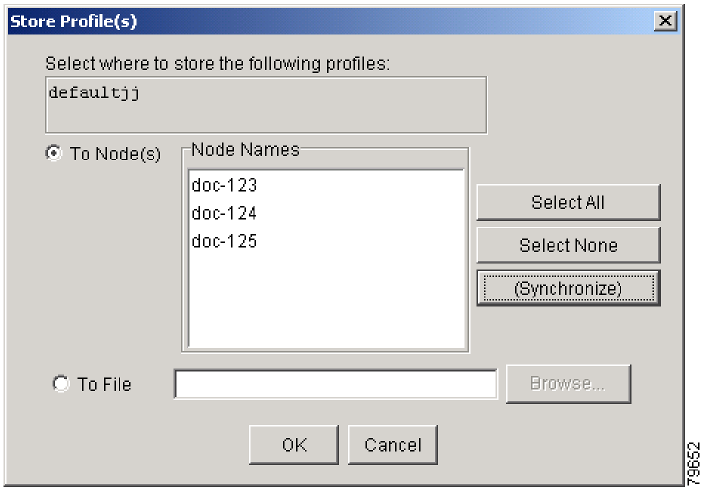
The downloaded profile appears on the right side of the Alarm Profiles tab.

Step 7 Right-click anywhere in the downloaded profile column to display the profile editing shortcut menu.

Step 8 Choose **Store** from the menu.

Step 9 In the Store Profile(s) dialog box, click the *To Node(s)* radio button (Figure 7-16).

Figure 7-16 Store Profile(s) dialog window



Store Profile(s)

Select where to store the following profiles:

defaultjj

● To Node(s)

Node Names

doc-123
doc-124
doc-125

○ To File

Step 10 Choose the node where you are logged on from the Node Names list, and click one of the following buttons:

- *Select All*—Selects all node names in the Node Names list. (This will also select all nodes if none are highlighted in the list.)
- *Select None*—Selects none of the node names in the Node Names list. (This will also select none of the nodes in the list even if they have been highlighted.)
- *(Synchronize)*—Synchronizes the stored alarm profile on the selected nodes.
- Click **OK**.

Step 11 Return to your originating procedure (NTP).

DLP-116 Apply Alarm Profiles to Ports

Purpose	Use this task to apply a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-115 Create Alarm Severity Profiles, page 7-17 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the node (default login) view, double-click a card to display the card view.

Note You can also apply alarm profiles to cards using the "DLP-117 Apply Alarm Profiles to Cards and Nodes" task on page 7-26.

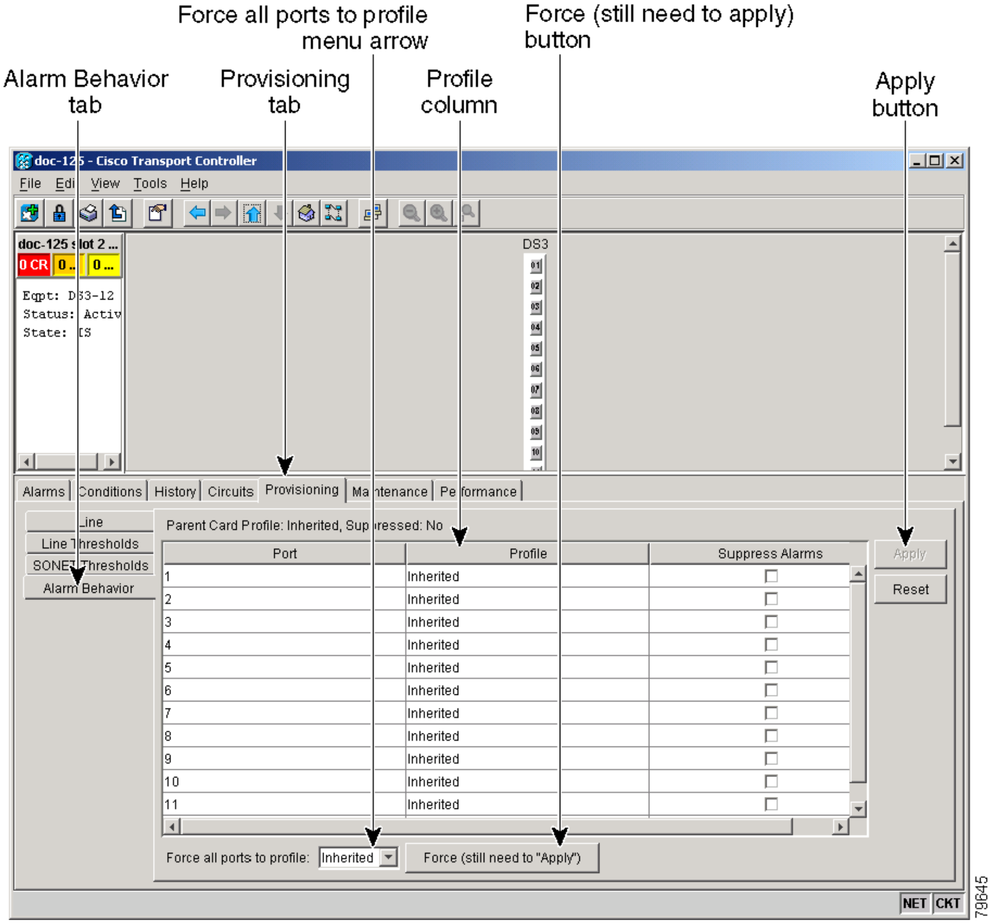
Note The card view is not available for the TCC+ or cross-connect cards.

Step 2 Click the **Provisioning > Alarm Behavior** tabs.

Figure 7-17 shows the profile of the affected DS-3 card. CTC shows Parent Card Profile: Inherited.

Go to Step 3 to apply profiles on a port-by-port basis. Go to Step 4 to apply profiles to all ports on a card.

Figure 7-17 Card view of a DS3 alarm profile



Eqpt: DS3-12
Status: Activ
State: IS

Parent Card Profile: Inherited, Suppressed: No

Port	Profile	Suppress Alarms
1	Inherited	□
2	Inherited	□
3	Inherited	□
4	Inherited	□
5	Inherited	□
6	Inherited	□
7	Inherited	□
8	Inherited	□
9	Inherited	□
10	Inherited	□
11	Inherited	□

Force all ports to profile: Inherited

Step 3 To apply profiles on a port basis:

a. Click the appropriate row under the Profile column for the port desired.

b. Choose the appropriate profile from the pull-down menu.

c. Click the **Apply** button.

Step 4 To apply profiles to all ports on a card:

a. Click the **Force all ports to profile** menu arrow at the bottom of the window.

b. Choose the appropriate profile from the pull-down menu.

c. Click the **Force (still need to "Apply")** button.

d. Click the **Apply** button

Step 5 Return to your originating procedure (NTP).

Tip If you choose the wrong profile, click **Reset** to return to the previous profile setting.

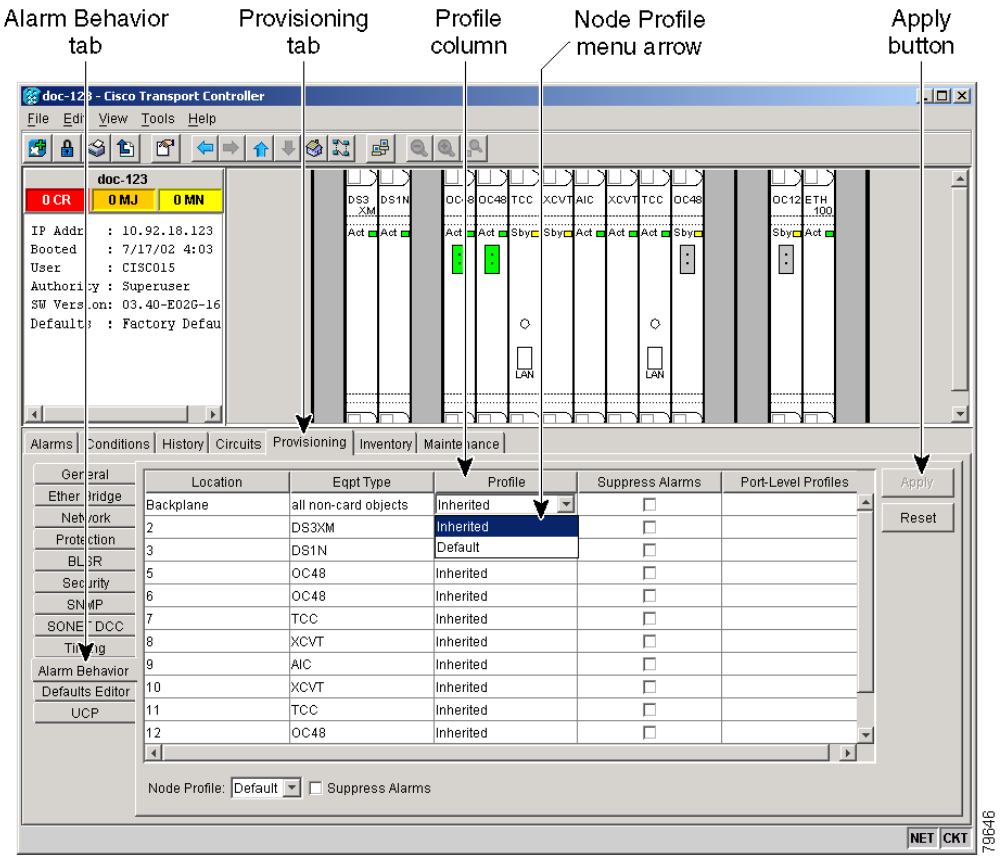
DLP-117 Apply Alarm Profiles to Cards and Nodes

Purpose	Use this task to apply a custom alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-115 Create Alarm Severity Profiles, page 7-17 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provision

Step 1 On the node (default login) view, click the **Provisioning > Alarm Behavior** tabs (Figure 7-18 on page 7-26).

To apply profiles on a card basis, go to Step 2. To apply the profile to the entire node, go to Step 3.

Figure 7-18 Node (default login) view of a DS3 alarm profile



IP Addr : 10.92.18.123
Booted : 7/17/02 4:03
User : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults : Factory Defau

Location	Eqpt Type	Profile	Suppress Alarms	Port-Level Profiles
Backplane	all non-card objects	Inherited	☐	
2	DS3XM	Inherited	☐	
3	DS1N	Default	☐	
5	OC48	Inherited	☐	
6	OC48	Inherited	☐	
7	TCC	Inherited	☐	
8	XCVT	Inherited	☐	
9	AIC	Inherited	☐	
10	XCVT	Inherited	☐	
11	TCC	Inherited	☐	
12	OC48	Inherited	☐	

Node Profile: Default ☐ Suppress Alarms

Step 2 To apply profiles on a card-by-card basis:

a. Click the Profile row for the card desired.

b. Choose the appropriate profile.

- c. Click **Apply**.
- d. Go to Step 4.

Step 3 To apply the profile to an entire node:

- a. Click the **Node Profile** menu arrow.
- b. Choose the appropriate Profile.
- c. Click **Apply**.
- d. Go to Step 4.

Step 4 Return to your originating procedure (NTP).

Tip If you choose the wrong profile, click Reset to return to the previous profile.

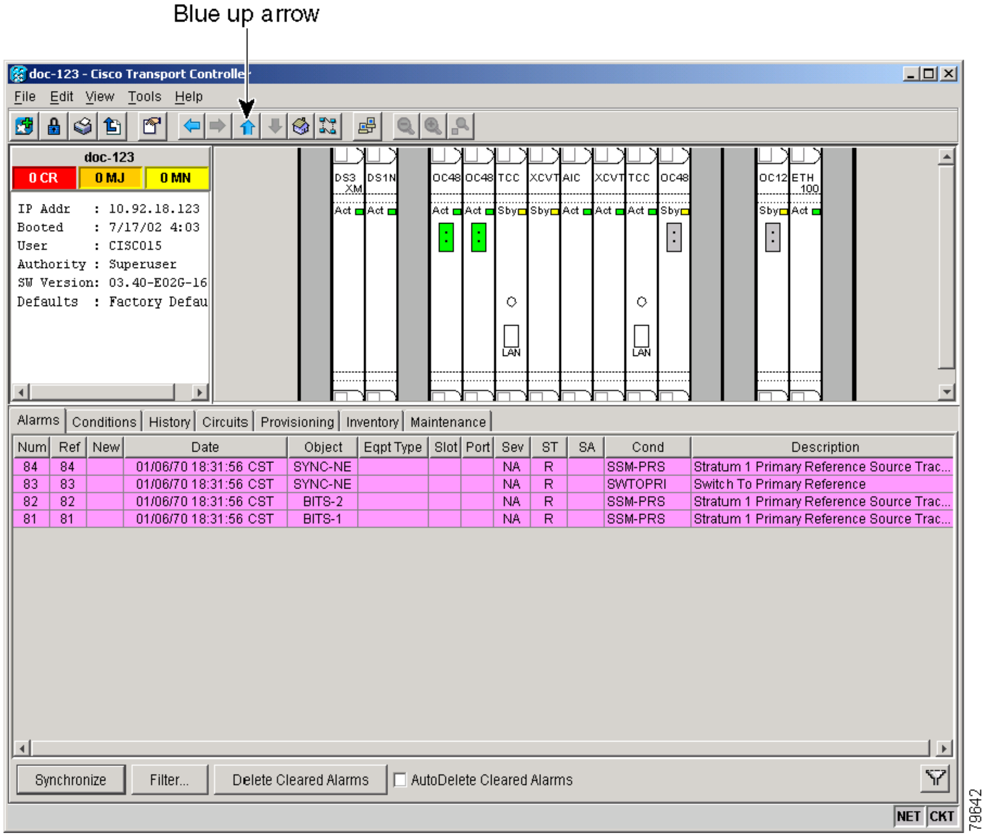
DLP-118 Delete Alarm Severity Profiles

Purpose	Use this task to delete a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provision

Step 1 From the node (default login) view, click the blue up arrow tool to display the network view.

Figure 7-19 shows the blue up arrow tool on the node (default login) view.

Figure 7-19 Blue up arrow tool on node (default login) view



```
IP Addr   : 10.92.18.123
Booted    : 7/17/02 4:03
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
84	84		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
83	83		01/06/70 18:31:56 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
82	82		01/06/70 18:31:56 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
81	81		01/06/70 18:31:56 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

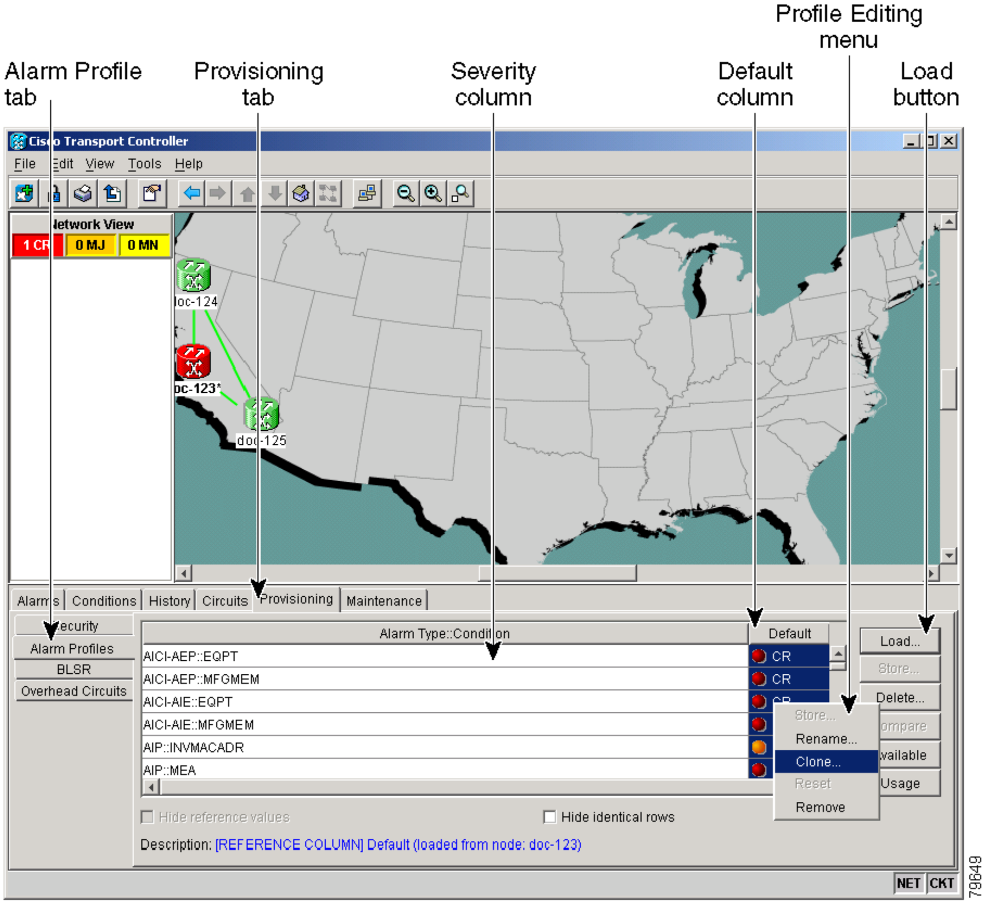
□ AutoDelete Cleared Alarms

Step 2 Click the **Provisioning > Alarm Profiles** tabs.

Step 3 Click the heading of the profile column you want to delete to highlight the profile column.

Figure 7-20 on page 7-29 shows the highlighted profile column.

Figure 7-20 Highlighted Alarm Profile column



Alarm Type::Condition	Default
AICI-AEP::EQPT	CR
AICI-AEP::MFGMEM	CR
AICI-AIE::EQPT	CR
AICI-AIE::MFGMEM	
AIP::INVMACADR	
AIP::MEA	

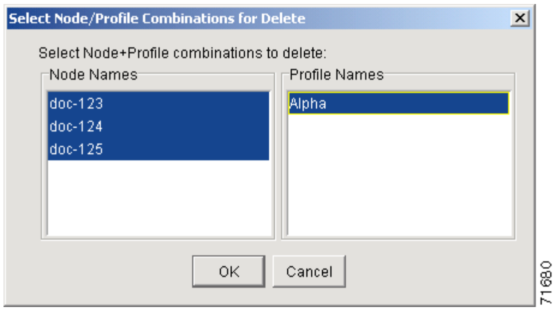
□ Hide reference values □ Hide identical rows

Description: [REFERENCE COLUMN] Default (loaded from node: doc-123)

Step 4 Click the **Delete** button.

The Select Node/Profile Combination for Delete dialog window appears (Figure 7-21).

Figure 7-21 Select Node/Profile Combination for Delete Window



Select Node+Profile combinations to delete:

Node Names: doc-123, doc-124, doc-125

Profile Names: Alpha

Step 5 Click the node name(s) in the Node Names list to highlight the nodes you want to delete profiles from. Hold down the Shift key to select multiple node names.

Step 6 Click the profile name(s) in the Profile Names list to highlight the profiles you want to delete from the highlighted node names.

Step 7 Click **OK**.

The Delete Alarm Profile confirmation dialog(s) appear.

Step 8 Click **Yes** for each Delete Alarm Profile confirmation dialog.

The profiles are now deleted from the nodes selected.

Step 9 If you want to also remove the profile from appearing on the Provisioning > Alarm Profiles tab, right-click the column of the profile you deleted, and choose **Remove** on the shortcut menu.

Step 10 Return to your originating procedure (NTP).

Note If a combination of node and profile are selected that do 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 and the user tries to delete from node A both profile 1 and profile 2, which exists only on nodes other than node A, this warning will appear. However, the operation still removes profile 1 from node A.

Note Deleting profiles currently in use prompts the user for a confirmation.

Note The special profiles called Default and Inherited may not be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

NTP-168 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	Use this procedure to enable, disable, or modify alarm severity filtering for alarms, conditions, or events 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 Log into a node where you want to create an enable alarm severity filtering. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 As necessary, complete the "DLP-225 Enable Alarm Filtering" task on page 7-31. 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-226 Modify Alarm and Condition Filtering Parameters" procedure on page 7-32. This task modifies the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-227 Disable Alarm Filtering" task on page 7-36. this task disables alarm profile filtering for all network nodes.

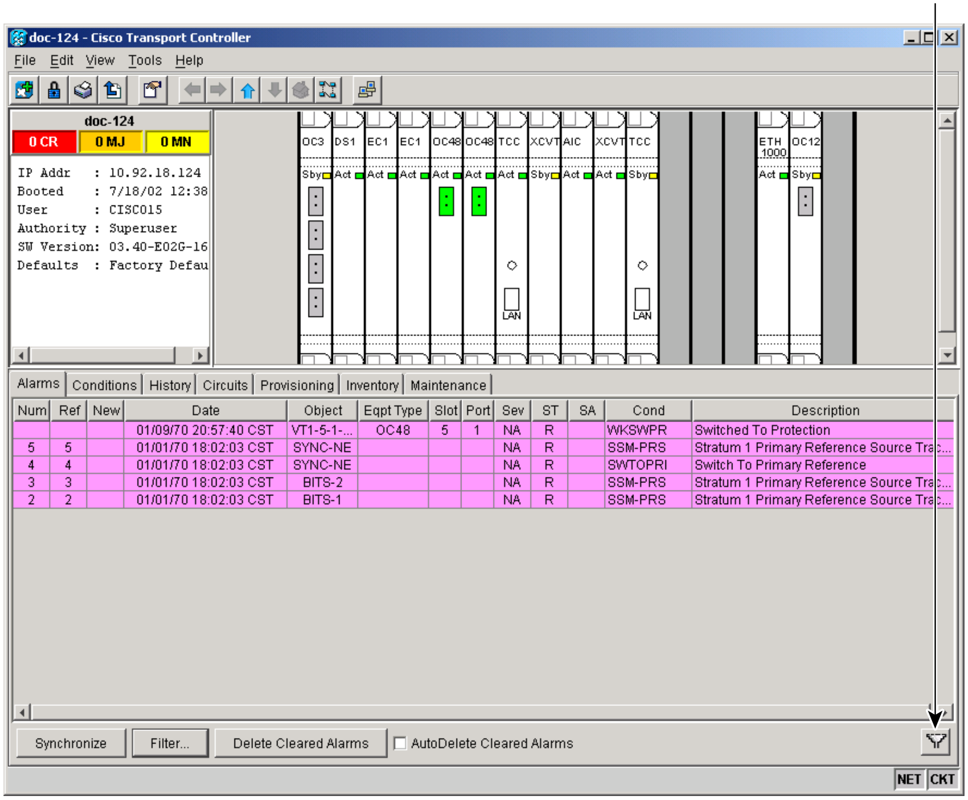
DLP-225 Enable Alarm Filtering

Purpose	Use this task to enable alarm filtering for alarms, conditions, or events 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 At the node, network, or card-level view, click the **Alarms** tab (Figure 7-22).

Figure 7-22 Node-level view of Alarms tab

Alarm Filtering tool



doc-124 - Cisco Transport Controller

doc-124

0 CR | 0 MJ | 0 MN

```
IP Addr   : 10.92.18.124
Booted    : 7/18/02 12:38
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
			01/09/70 20:57:40 CST	VT1-5-1-...	OC48	5	1	NA	R		WKSWPR	Switched To Protection
5	5		01/01/70 18:02:03 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
4	4		01/01/70 18:02:03 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
3	3		01/01/70 18:02:03 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
2	2		01/01/70 18:02:03 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

File Edit View Tools Help
OC3 DS1 EC1 EC1 OC48 OC48 TCC XCVT AIC XCVT TCC ETH 1000 OC12
Sby Act Act Act Act Act Act Sby Act Act Sby Act Sby
LAN
LAN
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Synchronize
Filter...
Delete Cleared Alarms
□ AutoDelete Cleared Alarms
NET CKT
78672

Step 2 Click the **Alarm Filter** tool at the lower-right side of the window bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is 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 tab.

Step 4 If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History tab.

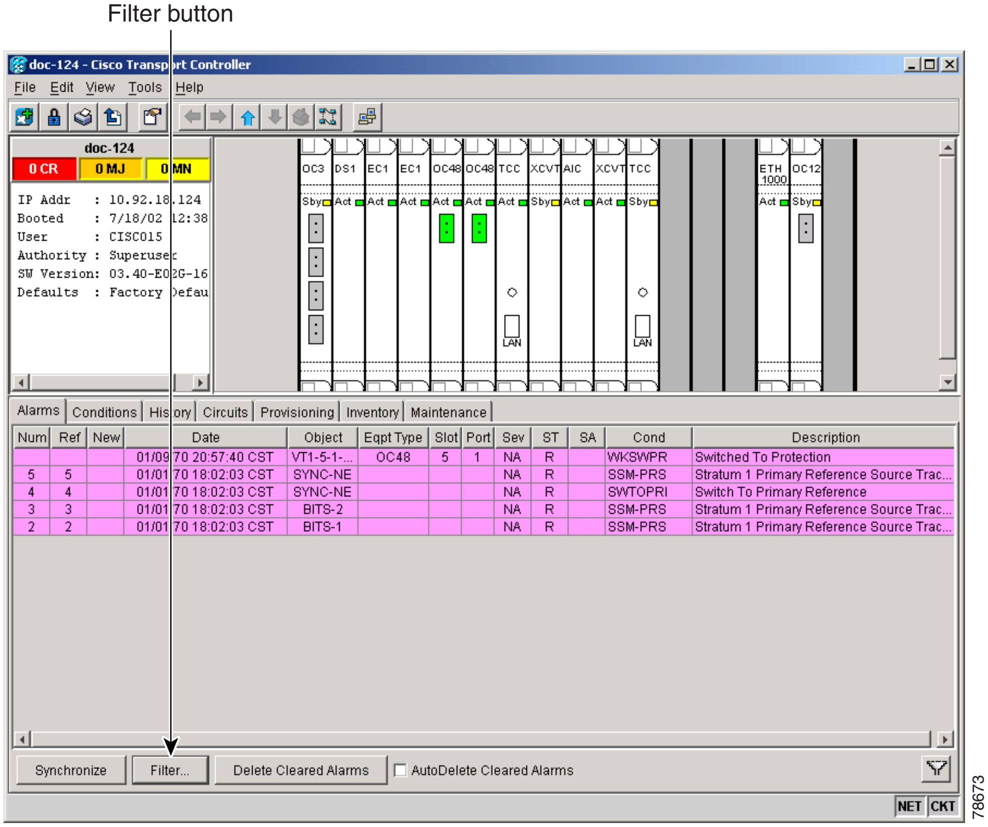
Step 5 Return to your originating procedure (NTP).

DLP-226 Modify Alarm and Condition Filtering Parameters

Purpose	Use this task to modify alarm filtering for alarms, conditions, or events in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-225 Enable Alarm Filtering, page 7-31
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card-level view, click the **Alarms** tab (Figure 7-23 on page 7-33).

Figure 7-23 Node-level view of Alarms tab



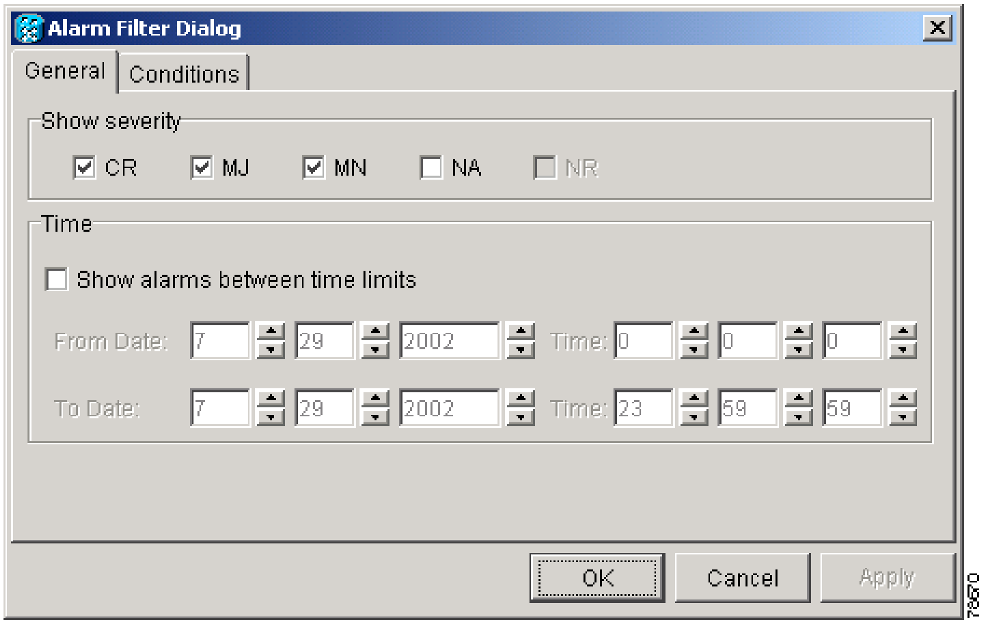
```
IP Addr   : 10.92.18.124
Booted    : 7/18/02 12:38
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
			01/09 70 20:57:40 CST	VT1-5-1-...	OC48	5	1	NA	R		WKSWPR	Switched To Protection
5	5		01/01 70 18:02:03 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
4	4		01/01 70 18:02:03 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
3	3		01/01 70 18:02:03 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
2	2		01/01 70 18:02:03 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

Step 2 Click the **Alarm Filter** tool at the lower-left side of the window bottom toolbar.

The Alarm Filter Dialog window appears, showing the General tab (Figure 7-24 on page 7-34).

Figure 7-24 Alarm Filter Dialog window, General tab



Show severity

☑ CR ☑ MJ ☑ MN ☐ NA ☐ NR

Time

☐ Show alarms between time limits

From Date: 7 29 2002 Time: 0 0 0

To Date: 7 29 2002 Time: 23 59 59

In the General tab Show Severity area, you can modify which alarm severities show through the alarm filter or the period of time to apply to the alarms. If you want to change the alarm severities shown in the filter, go to Step a. In the Time area, you can choose a time period that alarms are displayed for. If you want to change the time period that the alarms show for, go to Step b.

a. In the Show Severity area, click the checkboxes for critical (CR), major (MJ), minor (MN), or not alarmed (NA) to determine which alarms will bypass the alarm filter when it is enabled. Leave severity checkboxes empty to filter the alarms.

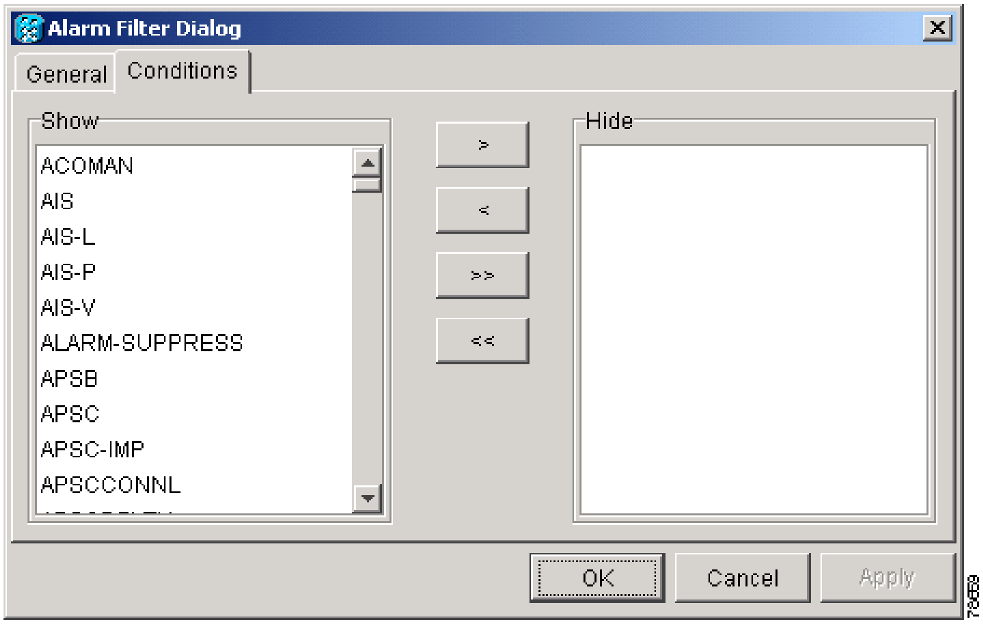
When alarm filtering is disabled, all alarms show.

b. In the Time area, click the **Show alarms between time limits** checkbox to enable it. Then click the up and down arrows in the From Date, To Date, and Time fields to modify what period of alarms will be shown.

Step 3 To modify filter parameters for conditions, proceed to Step 4. If not, proceed to Step 5.

Step 4 Click the Conditions tab (Figure 7-25 on page 7-35).

Figure 7-25 Alarm Filter Dialog window, Conditions tab



Alarm Filter Dialog

General | Conditions

Show:
- ACOMAN
- AIS
- AIS-L
- AIS-P
- AIS-V
- ALARM-SUPPRESS
- APSB
- APSC
- APSC-IMP
- APSCCONNL

Hide

Conditions in the Show list are visible when alarm filtering is enabled. Conditions in the Hide list are invisible when alarm filtering is enabled. 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 5 Click **Apply** and **OK**.

Filter parameters for alarms and conditions are enforced when alarm filtering is enabled, and not enforced when alarm filtering is disabled.

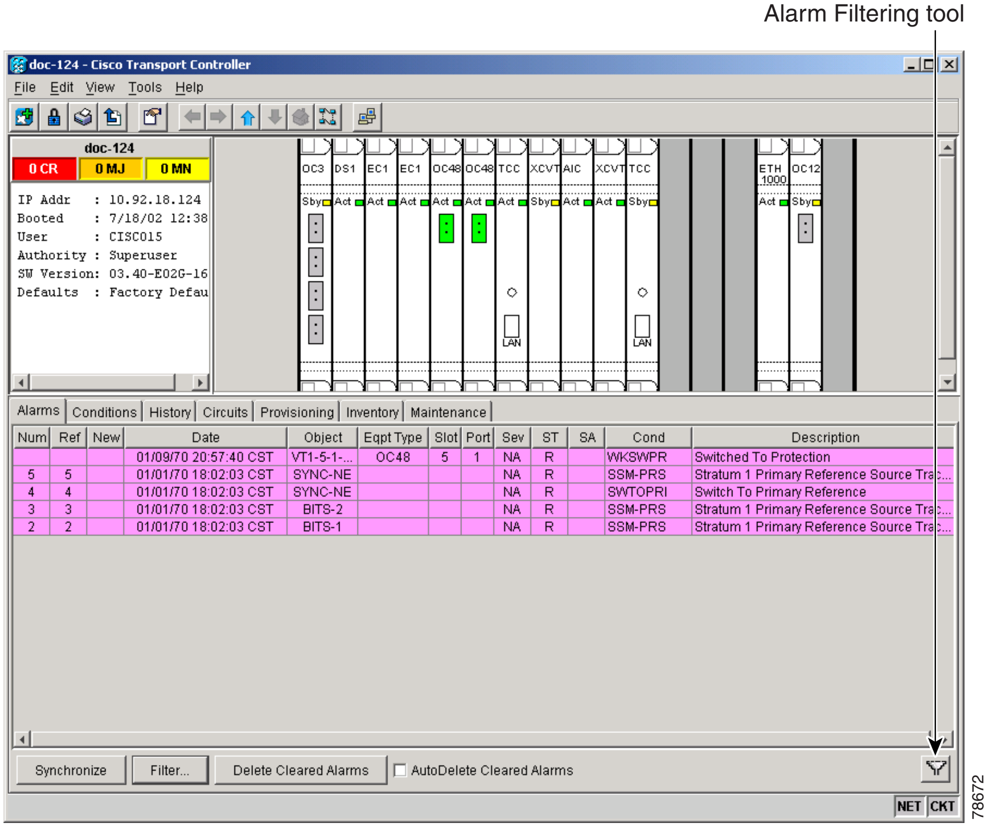
Step 6 Return to your originating procedure (NTP).

DLP-227 Disable Alarm Filtering

Purpose	Use this task to disable alarm filtering for alarms, conditions, or events in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-225 Enable Alarm Filtering, page 7-31
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the node, network, or card-level view, click the **Alarms** tab (Figure 7-26).

Figure 7-26 Node-level view of Alarms tab



Alarm Filtering tool
doc-124 - Cisco Transport Controller
File Edit View Tools Help
doc-124
0 CR
0 MJ
0 MN
OC3 DS1 EC1 EC1 OC48 OC48 TCC XCVT AIC XCVT TCC ETH 1000 OC12
Sby Act Act Act Act Act Act Sby Act Act Sby Act Sby
LAN
LAN
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Synchronize
Filter...
Delete Cleared Alarms
□ AutoDelete Cleared Alarms
NET CKT
78672

```
IP Addr   : 10.92.18.124
Booted    : 7/18/02 12:38
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
			01/09/70 20:57:40 CST	VT1-5-1-...	OC48	5	1	NA	R		WKSWPR	Switched To Protection
5	5		01/01/70 18:02:03 CST	SYNC-NE				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
4	4		01/01/70 18:02:03 CST	SYNC-NE				NA	R		SWTOPRI	Switch To Primary Reference
3	3		01/01/70 18:02:03 CST	BITS-2				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...
2	2		01/01/70 18:02:03 CST	BITS-1				NA	R		SSM-PRS	Stratum 1 Primary Reference Source Trac...

Step 2 Click the **Alarm Filter** tool at the lower-right side of the window bottom toolbar.

Alarm filtering is enabled if the tool is selected, and disabled if the tool is not selected.

Step 3 If you want alarm filtering disabled when you view conditions, repeat Steps 1 and 2 using the Conditions tab.

Step 4 If you want alarm filtering disabled when you view alarm history, repeat Steps 1 and 2 using the History tab.

Step 5 Return to your originating procedure (NTP).

NTP-72 Suppress and Unsuppress Alarm Reporting

Purpose	Use this procedure to suppress reported alarms at the port, card, or node level and disable the suppress command to resume normal alarm reporting.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Log into the ONS 15454. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Complete the "DLP-119 Suppress Alarm Reporting" task on page 7-37 to provision the node to send out autonomous messages to clear any raised alarms.

Note Suppressing alarms prevents alarms from appearing on Alarm or History tabs or in any other clients. The suppressed alarms behave like events, which have their own NA severities, and appear on the Conditions tab. The suppressed alarms appear with their alarm severity, color code, and service-affecting status.

Step 3 Complete the "DLP-120 Unsuppress Alarm Reporting" task on page 7-39 to remove the suppress-alarms command and provision the node to send out autonomous messages to raise any actively suppressed alarms.

DLP-119 Suppress Alarm Reporting

Purpose	Use this task to suppress the reporting of ONS 15454 alarms at the port, card, or node level.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

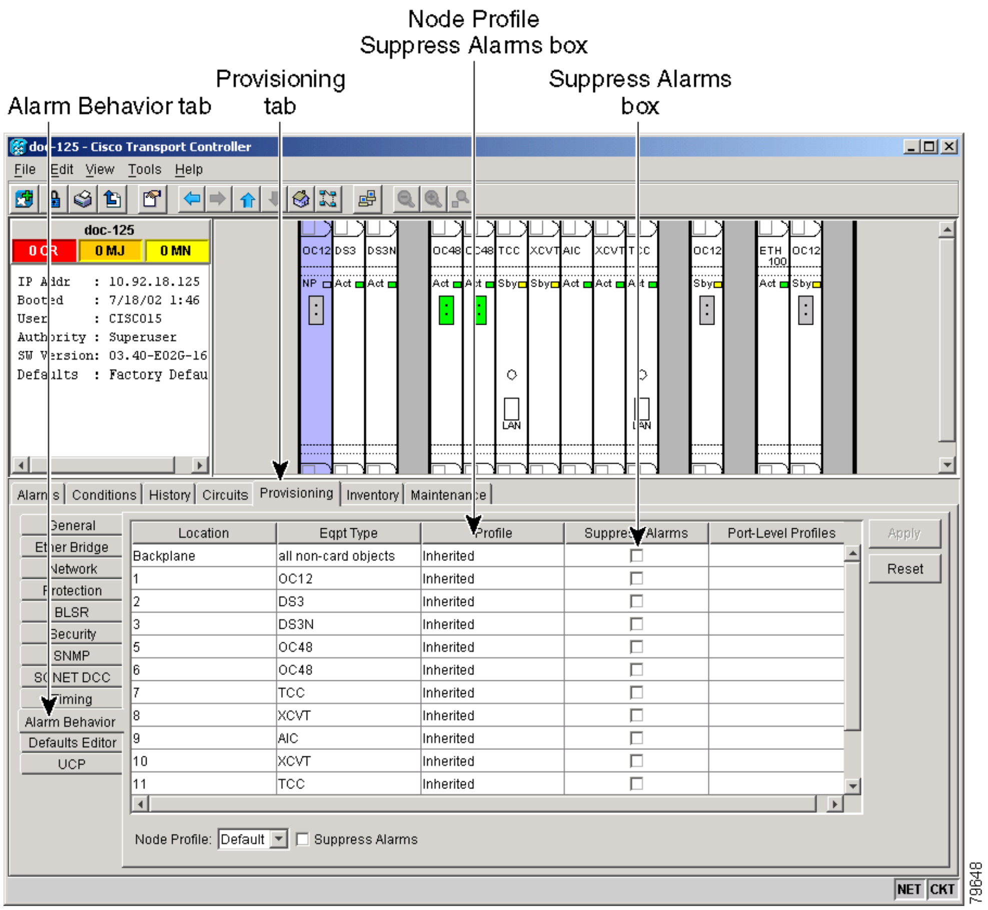
Step 1 At either the node (default) or card view, click the **Provisioning > Alarm Behavior** tabs.

At the card level, you can suppress alarms on a port-by-port basis. At the node level, you can suppress alarms on a card basis or on the entire node.

Step 2 Click the **Suppress Alarms** checkbox for the card (at the default login node view) or ports (at the card view) you want to suppress (Figure 7-27).

On the node (default login) view, row numbers correspond to slot numbers.

Figure 7-27 The Suppress Alarms checkbox


Node Profile
Suppress Alarms box
Provisioning tab
Suppress Alarms box
Alarm Behavior tab
doc-125 - Cisco Transport Controller
File Edit View Tools Help
doc-125
0 CR
0 MJ
0 MN
OC12 DS3 DS3N OC48 OC48 TCC XCVT AIC XCVT TCC OC12 ETH 100 OC12
NP Act Act Act Act Sby Sby Act Act Act Sby Act Sby
LAN
LAN
Alarms Conditions History Circuits Provisioning Inventory Maintenance
General
Ether Bridge
Network
Protection
BLSR
Security
SNMP
SONET DCC
Timing
Alarm Behavior
Defaults Editor
UCP
Apply
Reset
NET CKT
79648

```
IP Addr   : 10.92.18.125
Booted    : 7/18/02 1:46
User      : CISC015
Authority : Superuser
SW Version: 03.40-E02G-16
Defaults  : Factory Defau
```

Location	Eqpt Type	Profile	Suppress Alarms	Port-Level Profiles
Backplane	all non-card objects	Inherited	☐	
1	OC12	Inherited	☐	
2	DS3	Inherited	☐	
3	DS3N	Inherited	☐	
5	OC48	Inherited	☐	
6	OC48	Inherited	☐	
7	TCC	Inherited	☐	
8	XCVT	Inherited	☐	
9	AIC	Inherited	☐	
10	XCVT	Inherited	☐	
11	TCC	Inherited	☐	

Node Profile: Default ☐ Suppress Alarms

Step 3 Click the **Apply** button.

The node sends out autonomous messages to clear any raised alarms.

Step 4 Return to your originating procedure (NTP).

Caution If multiple CTC/TL1 sessions are open, suppressing alarms in one session will suppress the alarms in all other open sessions.

DLP-120 Unsuppress Alarm Reporting

Purpose	Use this task to discontinue alarm suppression and reenable alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-119 Suppress Alarm Reporting, page 7-37 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 At either the node (default) or card view, depending on where the alarms were suppressed, click the **Provisioning > Alarm Behavior** tabs.

Step 2 In card view, deselect the **Suppress Alarms** checkbox for the cards or ports you no longer want to suppress. In node (default login) view, deselect the Suppress Alarms checkbox next to the Node Profile field.

Step 3 Click the **Apply** button. The node sends out autonomous messages to raise any actively suppressed alarms.

Step 4 Return to your originating procedure (NTP).

CHAPTER 8

Monitor Performance

This chapter explains how to enable and view performance monitoring statistics for 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 for applicable tasks (DLPs).

1. NTP-73 Enable Performance Monitoring, page 8-1—Complete as needed.
2. NTP-74 Monitor Performance, page 8-6—Complete this procedure after enabling performance monitoring, as needed.

Note You can find additional PM information in the Digital transmission surveillance section in Telcordia's GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents, and in the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

NTP-73 Enable Performance Monitoring

Purpose	This procedure describes how to enable performance monitoring.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As Needed
Onsite/Remote	Either
Security Level	Provisioning and above

Step 1 Log into CTC at the node that you want to monitor. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Complete the "DLP-121 Enable Pointer Justification Count Performance Monitoring" task on page 8-2 if you need to monitor clock synchronization.

Step 3 Complete the "DLP-122 Enable Intermediate-Path Performance Monitoring" task on page 8-4 if you need to monitor large amounts of STS traffic through intermediate nodes.

DLP-121 Enable Pointer Justification Count Performance Monitoring

Purpose	This task enables pointer justification counts, which provide a way to align the phase variations in STS and VT payloads and to monitor the clock synchronization between nodes. A consistent, large pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	Before you view pointer justification PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, refer to Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Provisioning and above

Step 1 In node view, double-click the card where the line terminates (drops), called a line terminated equipment (LTE) card. The card view displays.

See Table 8-1 for a list of Cisco ONS 15454 LTE cards.

Table 8-1 Traffic Cards that Terminate the Line, Called LTEs

Line Terminating Equipment	
EC1-12	
DS1-14	DS1N-14
DS3-12	DS3N-12
DS3-12E	DS3N-12E
DS3XM-6	OC3 IR4 1310
OC12 IR 1310	OC12 LR 1310
OC12 LR 1550	Quad OC12
OC48 IR 1310	OC48 LR 1550
OC48 IR/STM16 SH AS 1310	OC48 LR/STM16 LH AS 1550
OC192 LR 1550	OC48 ELR 200 Ghz ITU
OC48 ELR 100 Ghz ITU	E100T-12
E1000-2	E100T-G
E1000-2-G	G1000-4

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Click the PJStsMon# menu and choose a number based on the following rules: Figure 8-1 shows the **PJStsMon#** menu on the Provisioning screen.

- The default value of 0 means pointer justification monitoring is disabled.
- The values 1-N are the number of STSs on the port. One STS per port can be enabled from the PJStsMon# card menu.

  In the card view for the EC1 card, choose 0 or 1 on each of 12 ports.

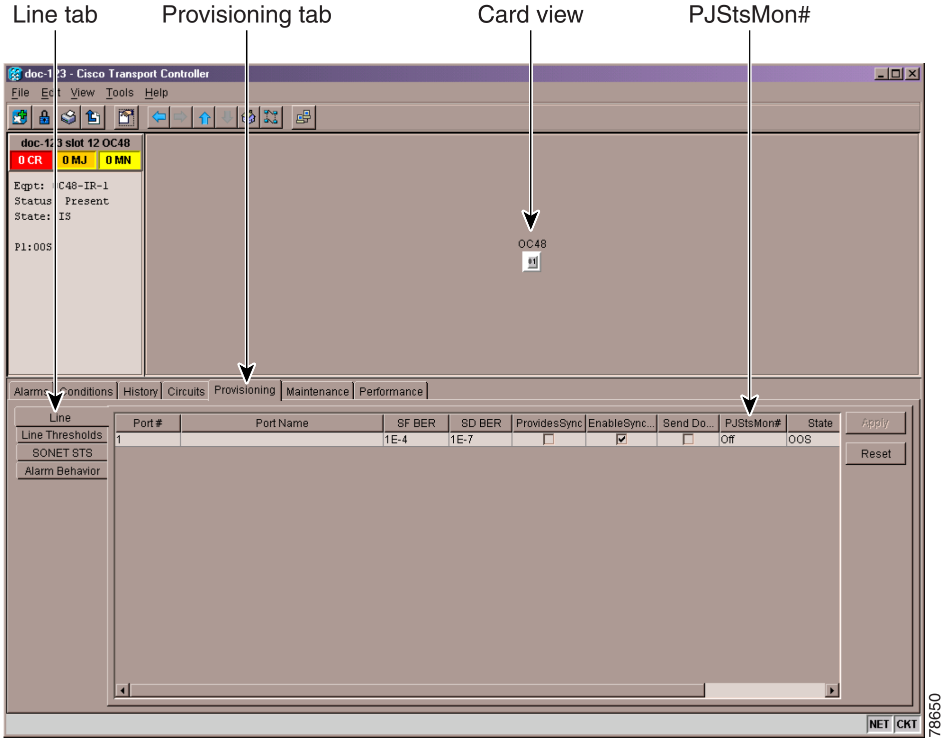
  In the card view for the OC-3 card, choose 0, or any number 1 through 3 on each port.

  In the card view for the OC-12 card, choose 0, or any number 1 through 12 on each port.

  In the card view for the OC-48 card, choose 0, or any number 1 through 48 on each port.

  In the card view for the OC-192 card, choose 0, or any number 1 through 192 on each port.

Figure 8-1 Line tab for enabling pointer justification count parameters



```
Eqpt:  OC48-IR-1
Status  Present
State: IS

P1:OOS
```

Port #	Port Name	SF BER	SD BER	ProvidesSync	EnableSync...	Send Do...	PJStsMon#	State
1		1E-4	1E-7	□	☑	□	Off	OOS

Step 4 Confirm that the port is In Service.

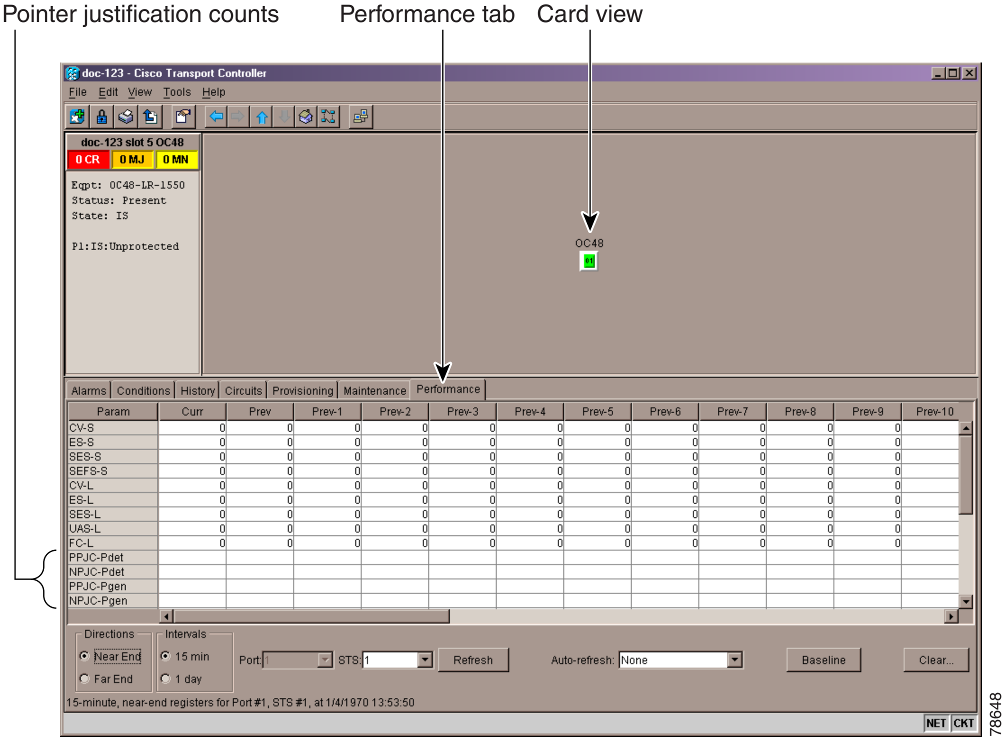
Step 5 If the port is In Service, click **Apply** and go to Step 7.

Step 6 If the port is Out of Service, select **In Service** in the Status field and click Apply.

Step 7 Click the **Performance** tab to view PM parameters. Figure 8-2 shows pointer justification count. Refer to the *Cisco ONS 15454 Reference Guide* for more PM information, details, and definitions.

Note On CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs.

Figure 8-2 Viewing Pointer Justification Counts



Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1 STS: 1
Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

DLP-122 Enable Intermediate-Path Performance Monitoring

Note The monitored IPPMs are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. For more information about IPPM, see the *Cisco ONS 15454 Reference Guide*.

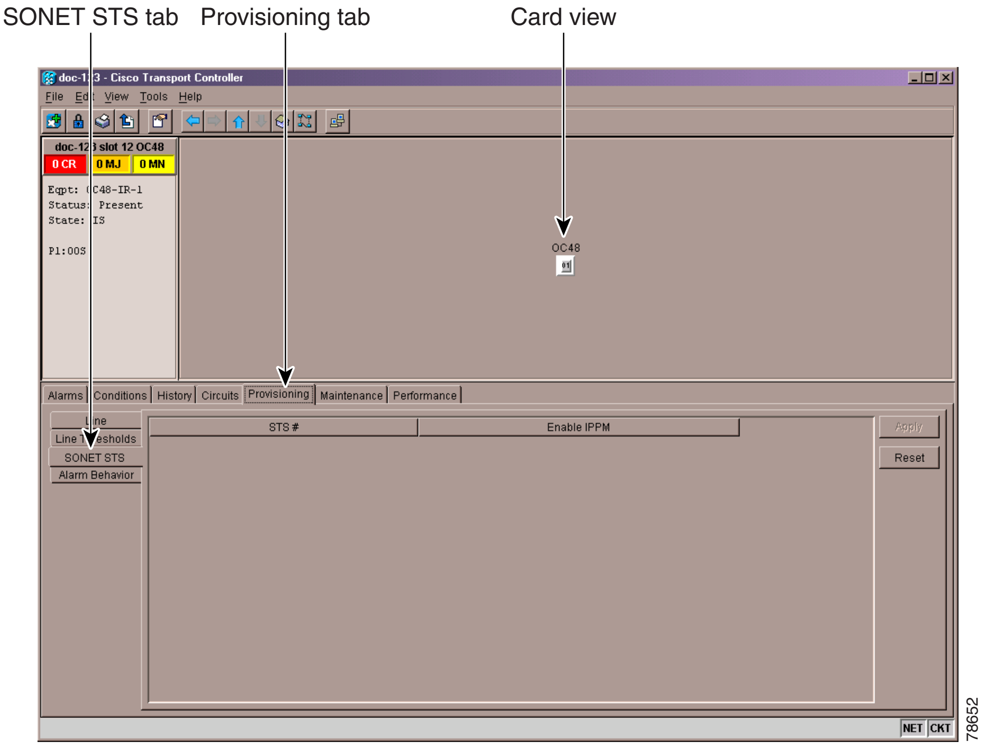
Purpose	This task enables intermediate-path performance monitoring, which allows you to monitor large amounts of STS traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	If no STS circuit exists, use Chapter 6, "Create Circuits and VT Tunnels" to create an STS circuit. The circuit must pass through the EC-1 or OC-N card before you can enable IPPM on the circuit.
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Provisioning and above

Step 1 In node view, double-click the LTE card you want to monitor. The card view displays.

See Table 8-1 on page 8-2 for a list of Cisco ONS 15454 LTE cards.

Step 2 Click the **Provisioning > SONET STS** tabs. Figure 8-3 shows the SONET STS tab on the Provisioning screen.

Figure 8-3 SONET STS tab for enabling IPPM



Eqpt: OC48-IR-1
Status: Present
State: IS

P1:OOS

Step 3 Click **Enable IPPM** for the STS you want to monitor and click **Apply**.

Step 4 Click the **Performance** tab to view PM parameters. For IPPM definitions refer to the *Cisco ONS 15454 Reference Guide*.

NTP-74 Monitor Performance

Purpose	The Performance Monitoring screen allows you to monitor node performance in 15-minute intervals or 24-hour periods and to monitor near-end PMs or far-end PMs.
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 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Log into CTC at the node that you want to monitor. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Complete the "DLP-123 View PMs" task on page 8-6.

Step 3 As needed, use the following tasks to change the display of PM counts:

- "DLP-124 Refresh PM Counts at Fifteen-Minute Intervals" task on page 8-7
- "DLP-125 Refresh PM Counts at Twenty-Four Hour Intervals" task on page 8-9
- "DLP-126 Monitor Near-End PM Counts" task on page 8-10
- "DLP-127 Monitor Far-End PM Counts" task on page 8-11
- "DLP-128 Monitor PM Counts for Near-End or Far-End Signals" task on page 8-13
- "DLP-129 Reset Current PM Counts" task on page 8-14
- "DLP-130 Clear Selected PM Counts" task on page 8-16

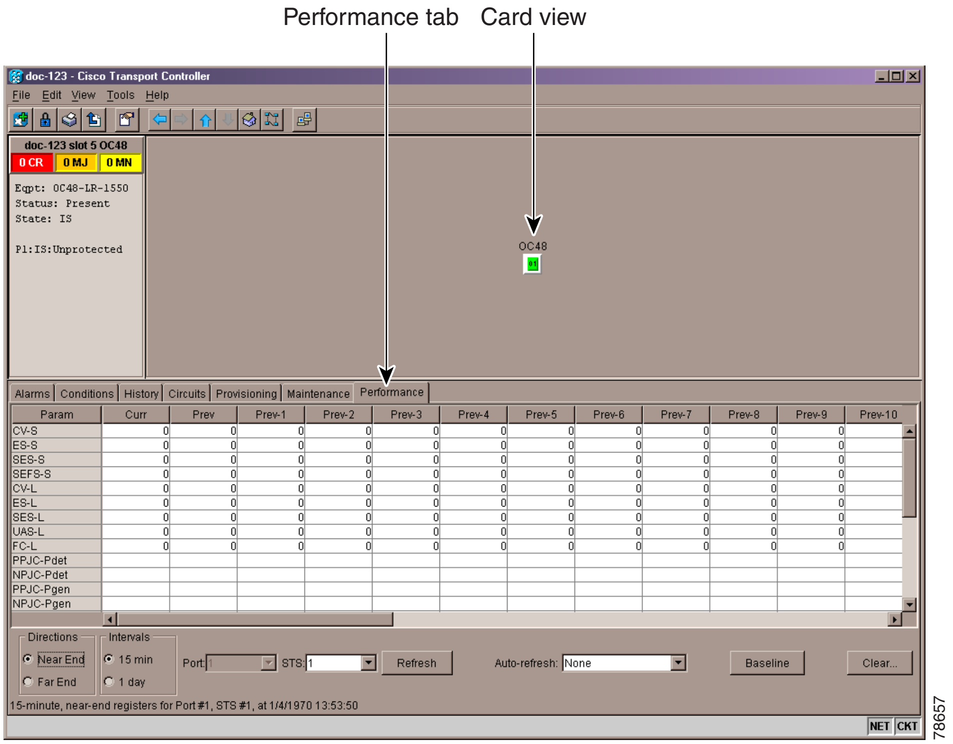
DLP-123 View PMs

Purpose	This task enables you to view PM counts to detect performance problems early.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab (Figure 8-4).

Figure 8-4 Viewing performance monitoring information



doc-123 slot 5 OC48
0 CR 0 MJ 0 MN

Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1 STS: 1 Refresh
Auto-refresh: None
Baseline Clear...

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 3 View the PM parameter names that appear on the left portion of the screen in the Param column. The parameter numbers appear on the right portion of the screen in the Curr (current), and Prev (previous) columns. For PM definitions refer to the *Cisco ONS 15454 Reference Guide*.

Step 4 Return to your originating procedure (NTP).

DLP-124 Refresh PM Counts at Fifteen-Minute Intervals

Purpose	This task changes the screen view to display PMs in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, “Create Circuits and VT Tunnels” and Chapter 11, “Change Card Settings.”
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

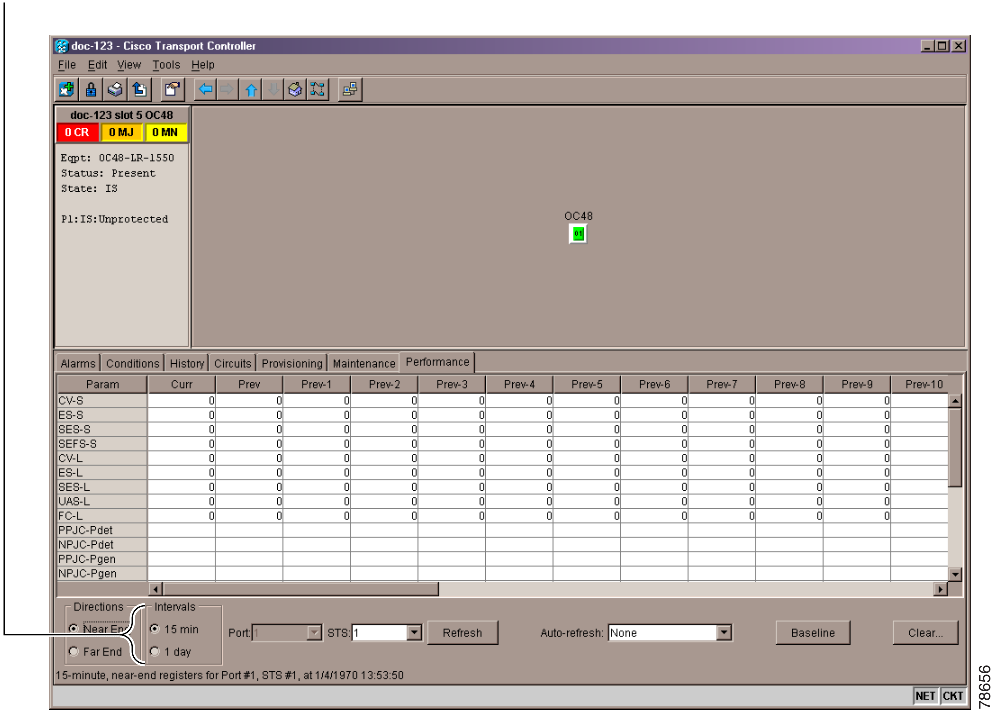
Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** button. Figure 8-5 shows the time interval buttons on the Performance Monitoring screen.

Figure 8-5 Time interval buttons on the card view Performance tab

Fifteen-minute and twenty-four hour interval buttons



```
Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1 STS: 1
Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 Click the **Refresh** button. Performance monitoring parameters display 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) will be 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 preceding 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value displays 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 by 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-125 Refresh PM Counts at Twenty-Four Hour Intervals

Purpose	This task changes the screen view to display PMs in 24-hour periods.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

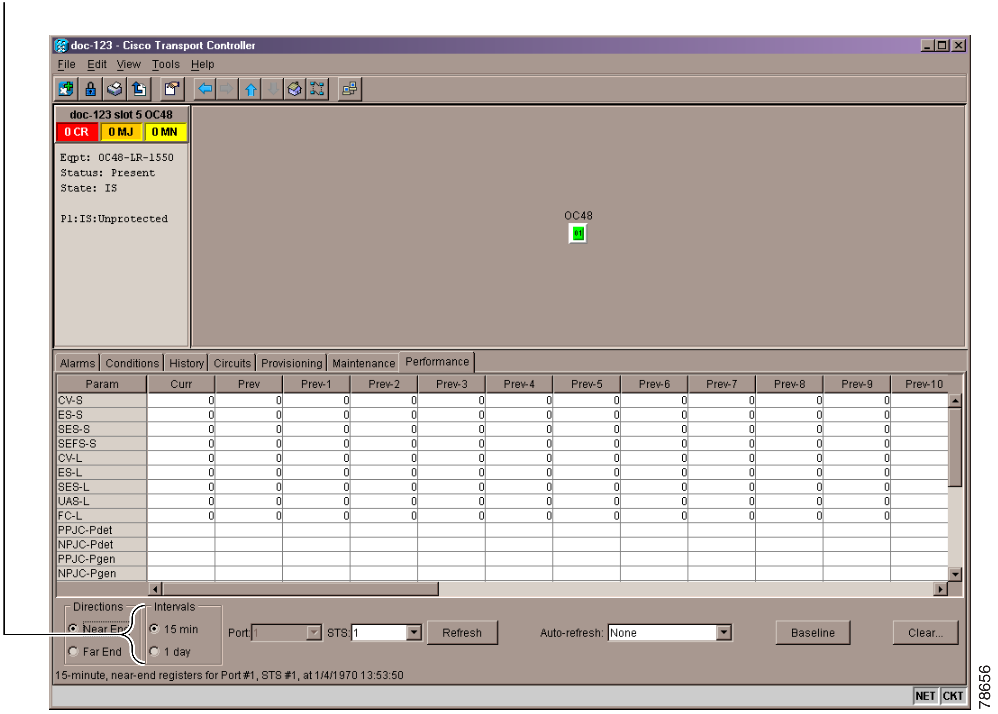
Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** button. Figure 8-6 shows the time interval buttons on the Performance Monitoring screen.

Figure 8-6 Time interval buttons on the card view Performance tab

Fifteen-minute and twenty-four hour interval buttons



doc-123 - Cisco Transport Controller

doc-123 slot 5 OC48

0 CR 0 MJ 0 MN

```
Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1 STS: 1

Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 Click the **Refresh** button. Performance monitoring displays in 24-hour periods synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 24-hour period.

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 24-hour period, a threshold crossing alert (TCA) will be raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev columns to find PM counts for the preceding 24-hour period.

Note If a complete count over a 24-hour period is not possible, the value displays 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 by changing port states. When the problem is corrected, the subsequent 24-hour period appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-126 Monitor Near-End PM Counts

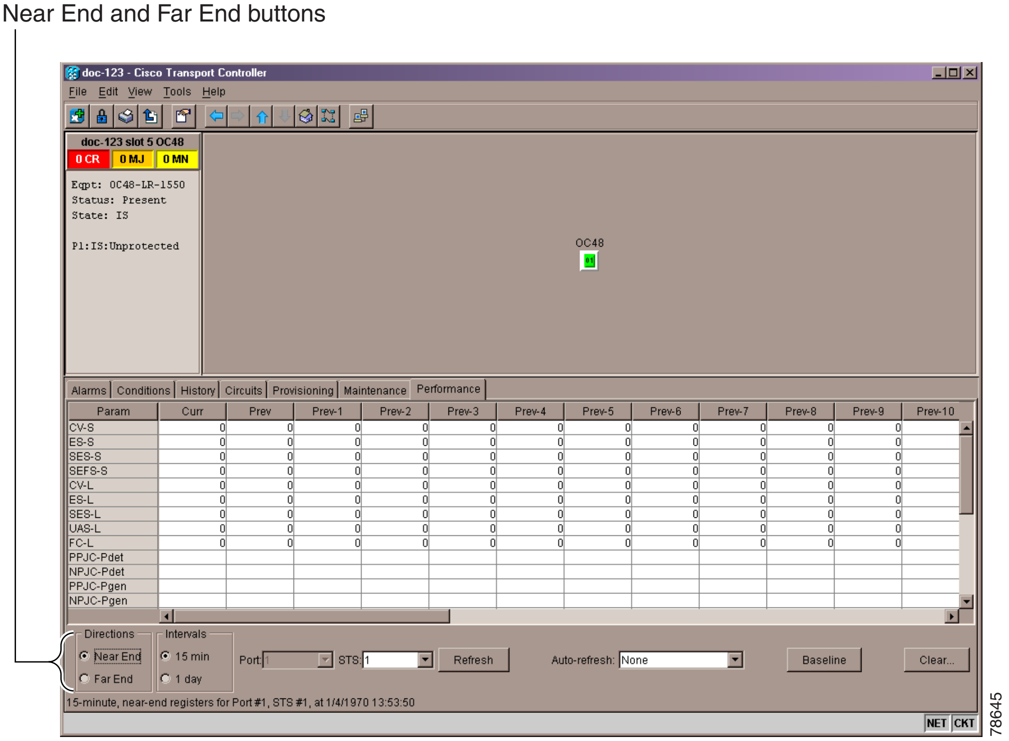
Purpose	Use this task to view PMs on the near end.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** button. Figure 8-7 shows the Near End and Far End buttons on the Performance Monitoring screen.

Figure 8-7 Near End and Far End buttons on the card view Performance tab



Near End and Far End buttons

Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1 STS: 1 Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 Click the **Refresh** button. All PMs occurring for the selected card on the incoming signal are displayed. For PM definitions refer to the *Cisco ONS 15454 Reference Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-127 Monitor Far-End PM Counts

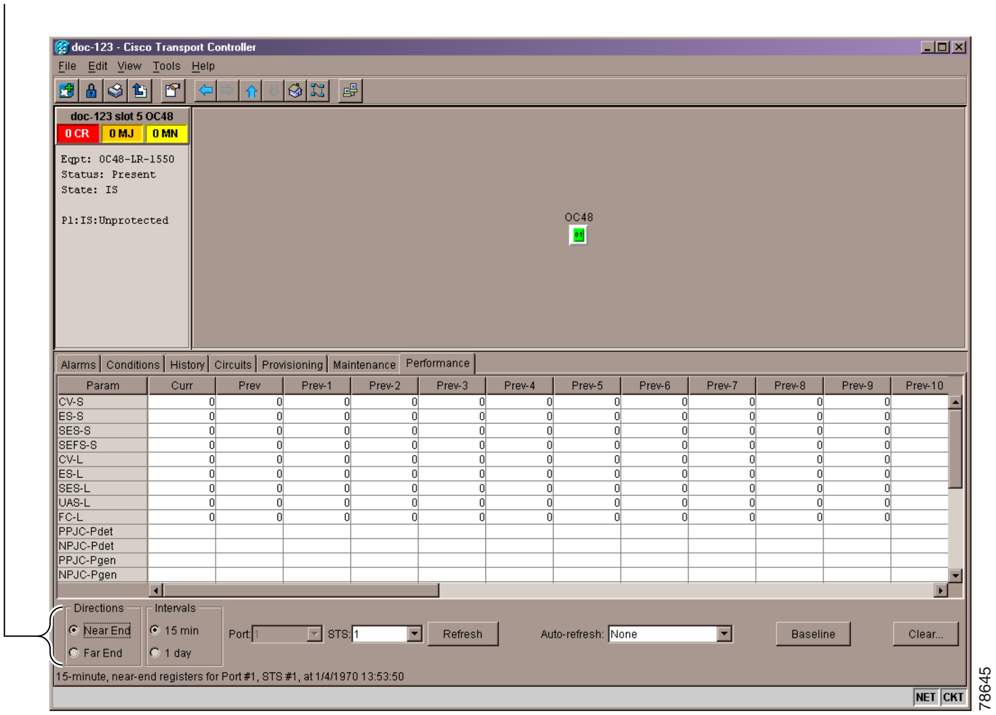
Purpose	Use this task to view PMs on the far end.
Tools/Equipment	None
Prerequisite Procedures	Only cards that allow far-end monitoring have this button as an option. Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** button. Figure 8-8 shows the Near End and Far End buttons on the Performance Monitoring screen.

Figure 8-8 Near End and Far End buttons on the card view Performance tab



doc-123 slot 5 OC48

0 CR | 0 MJ | 0 MN

```
Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1 STS: 1 Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 Click the **Refresh** button. All PMs recorded by the far-end node for the selected card on the outgoing signal are displayed. For PM definitions refer to the *Cisco ONS 15454 Reference Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-128 Monitor PM Counts for Near-End or Far-End Signals

Purpose	Use the signal-type menus to monitor PMs for near-end or far-end signals on a selected port.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

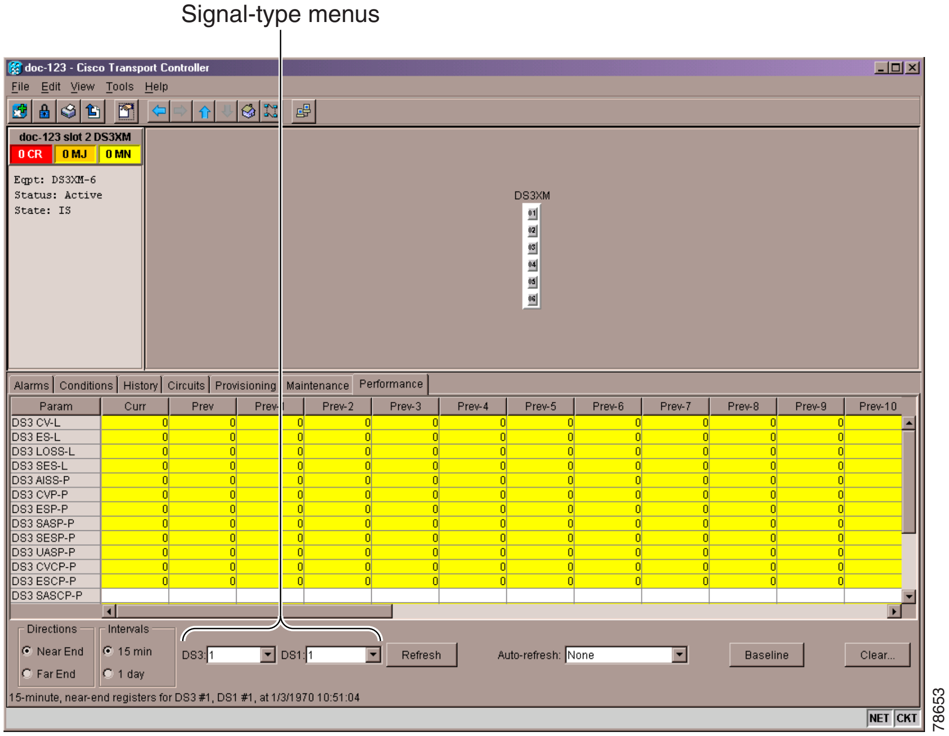
Step 2 Click the **Performance** tab.

Note Different signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OCn section, line) appear based on the card. For example, the DS3XM card lists DS3, DS1, VT path, and STS path PMs as signal-types.

Step 3 Click one of the signal-type menus labeled in Figure 8-9. Depending on the card, other options may be available (i.e. Port, STS, or VT).

For example, the DS3XM card allows a selection of both the DS-3 port and the DS-1 within the specified DS-3. Figure 8-9 shows the signal-type menus on the Performance Monitoring screen for a DS3XM-6 card.

Figure 8-9 Signal-type menus for a DS3XM-6 card



Eqpt: DS3XM-6
Status: Active
State: IS

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
DS3 CV-L	0	0	0	0	0	0	0	0	0	0	0	
DS3 ES-L	0	0	0	0	0	0	0	0	0	0	0	
DS3 LOSS-L	0	0	0	0	0	0	0	0	0	0	0	
DS3 SES-L	0	0	0	0	0	0	0	0	0	0	0	
DS3 AISS-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 CVP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 ESP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 SASP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 SESP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 UASP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 CVCP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 ESCP-P	0	0	0	0	0	0	0	0	0	0	0	
DS3 SASCP-P												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
DS3: 1 DS1: 1
Auto-refresh: None

15-minute, near-end registers for DS3 #1, DS1 #1, at 1/3/1970 10:51:04

Step 4 Click the **Refresh** button. All PMs recorded by the near-end or far-end node for the selected card on the outgoing signal on a selected port are displayed. For PM definitions refer to the *Cisco ONS 15454 Reference Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-129 Reset Current PM Counts

Purpose	The Baseline button clears the PM count displayed on the Curr column, but it does not clear the cumulative PM count. This allows you to see how quickly PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, "Create Circuits and VT Tunnels" and Chapter 11, "Change Card Settings."
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

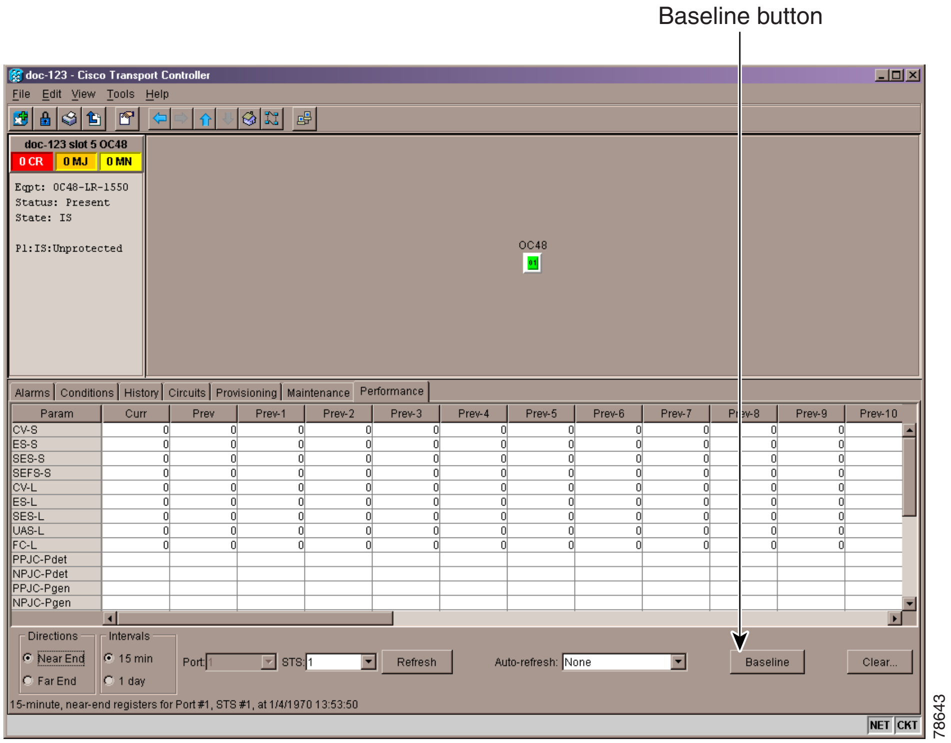
Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **Baseline** button. Figure 8-10 shows the Baseline button on the Performance Monitoring screen.

> **Note** The Baseline button clears the PM count displayed in the Curr column, but does not clear the PM count on the card. When the current 15-minute or 24-hour time interval expires or the screen view changes, the total number of PM counts on the card and on the screen appear in the appropriate column. The baseline values are discarded if you change views to a different screen and then return to the Performance Monitoring screen.

Figure 8-10 Baseline button for clearing displayed PM counts



Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1 STS: 1
Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 Return to your originating procedure (NTP).

DLP-130 Clear Selected PM Counts

Purpose	Use the Clear button to clear certain PM counts depending on the option selected.
Tools/Equipment	None
Prerequisite Procedures	Before you view or clear PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 6, “Create Circuits and VT Tunnels” and Chapter 11, “Change Card Settings.”
Required/As Needed	As needed
Onsite/Remote	Either
Security Level	Retrieve or higher

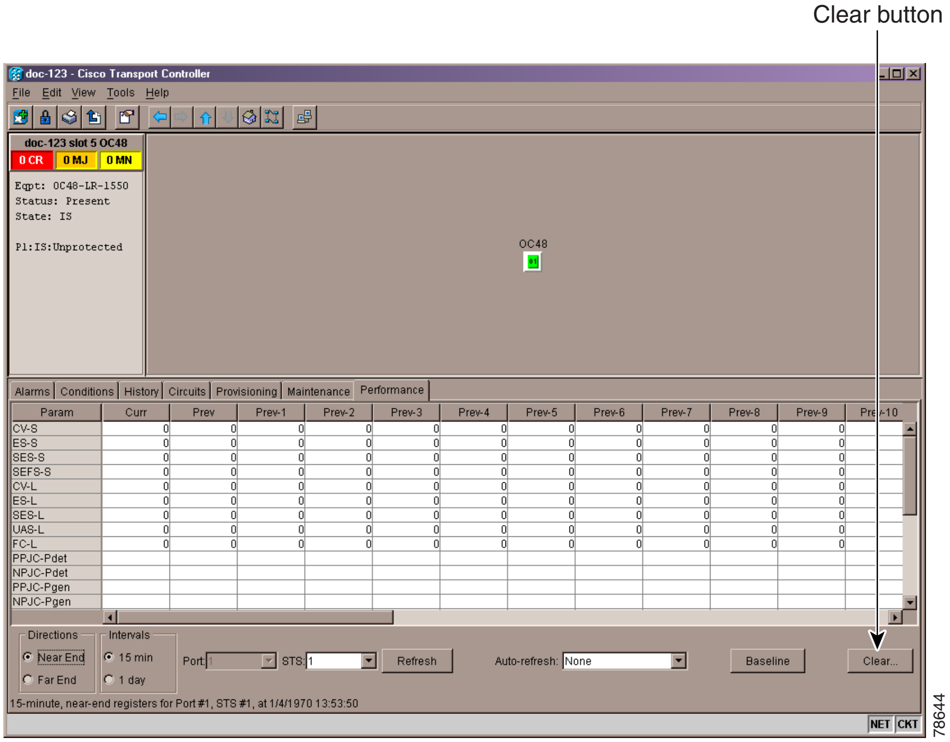
⚠ **Caution** Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click the electrical or optical (OC-N) card of choice. The card view displays.

Step 2 Click the **Performance** tab.

Step 3 Click the **Clear** button (Figure 8-11).

Figure 8-11 Clear button for clearing PM counts



Eqpt: OC48-LR-1550
Status: Present
State: IS

P1:IS:Unprotected

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Prev-10
CV-S	0	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	0	
CV-L	0	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	0	
PPJC-Pdet												
NPJC-Pdet												
PPJC-Pgen												
NPJC-Pgen												

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1 STS: 1
Auto-refresh: None

15-minute, near-end registers for Port #1, STS #1, at 1/4/1970 13:53:50

Step 4 From the Clear Statistics menu, choose one of three options:

- **Selected Interfaces**: Clearing selected interfaces erases all PM counts associated with the selected radio buttons. For example, if the 15 min and the Near End buttons are selected and you click the Clear button, all near-end PM counts in the current 15-minute interval are erased from the card and the screen display.
- **All interfaces on port x**: Clearing all interfaces on port x erases from the card and the screen display all PM counts associated with all combinations of the radio buttons on the selected port. This means the 15-minute near-end and far-end counts are cleared, and 24-hour near-end and far-end counts are cleared from the card and the screen display.
- **All interfaces on card**: Clearing all interfaces on the card erases from the card and the screen display all PM counts for all ports.

Step 5 From the Clear Statistics menu, click **Yes** to clear the selected statistics.

Step 6 Return to your originating procedure (NTP).

CHAPTER 9

Manage Circuits

This chapter explains how to manage Cisco ONS 15454 electrical, optical and Ethernet circuits.

Before You Begin

To create circuits, see Chapter 6, "Create Circuits and VT Tunnels."

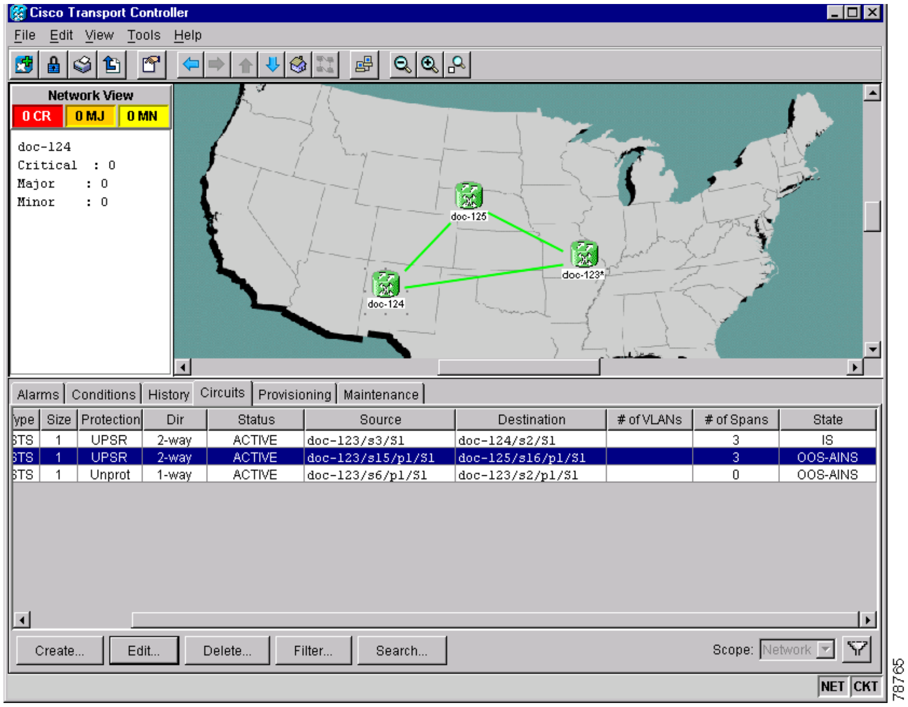
To clear any alarm or trouble conditions, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

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

1. NTP-150 Locate and View Circuits, page 9-3—Complete as needed.
2. NTP-151 Modify Circuit Characteristics, page 9-7—Complete as needed to edit a circuit name, change the active and standby colors of spans, or change signal fail, signal degrade thresholds, reversion time, and PDI-P settings for UPSR circuits.
3. NTP-152 Delete Circuits, page 9-11—Complete as needed.
4. NTP-78 Create a Monitor Circuit, page 9-12—Complete as needed to monitor traffic on primary bidirectional circuits.
5. NTP-79 Create a J1 Path Trace, page 9-13—Complete as needed to monitor interruptions or changes to circuit traffic.

The ONS 15454 Circuits window (Figure 9-1) displays information about circuits to help you manage the circuits. Two key attributes are status and state. Circuit status shown in Table 9-1, is CTC-generated information telling you what CTC has learned about the circuit. State, shown in Table 9-2, is a user-assigned, administrative status that defines whether the circuit is in or out of service. To carry circuit traffic, circuits must have a status of Active and a state of In Service (IS).

Figure 9-1 ONS 15454 Circuit window in network view



```
doc-124
Critical  : 0
Major     : 0
Minor     : 0
```

ype	Size	Protection	Dir	Status	Source	Destination	# of VLANs	# of Spans	State
STS	1	UPSR	2-way	ACTIVE	doc-123/s3/S1	doc-124/s2/S1		3	IS
STS	1	UPSR	2-way	ACTIVE	doc-123/s15/p1/S1	doc-125/s16/p1/S1		3	OOS-AINS
STS	1	Unprot	1-way	ACTIVE	doc-123/s6/p1/S1	doc-123/s2/p1/S1		0	OOS-AINS

Table 9-1 ONS 15454 Circuit Status

Status	Definition/Activity
CREATING	CTC-created circuit is being created
ACTIVE	CTC-created circuit is complete. All components are in place and a complete path exists from circuit source to destination.
DELETING	Circuit is being deleted
INCOMPLETE	CTC-created circuit is missing a connection or circuit span (network link); a complete path from source to destination(s) does not exist, or an AIP (MAC address) change occurred on one of the circuit nodes and the circuit is in need of repair.
UPGRADABLE	A TL1-created circuit is complete and has upgradable connections. A complete path from source to destination(s) exists. The circuit may be upgraded.
INCOMPLETE_UPGRADABLE	TL1-created circuit with upgradable connections is missing a connection or circuit span (network link), and a complete path from source to destination(s) does not exist. The circuit cannot be upgraded until missing components are in place.

Table 9-1 ONS 15454 Circuit Status

Status	Definition/Activity
NOT_UPGRADABLE	TL1-created circuit is complete but has at least one non-upgradable connection. UPSR_HEAD, UPSR_EN, UPSR_DC, and UPSR_DROP connections are not upgradable, so all unidirectional UPSR circuits created with TL1 are not upgradable.
INCOMPLETE_NOT_UPGRADABLE	TL1-created circuit with one or more non-upgradable connections is missing a connection or circuit span (network link); a complete path from source to destination(s) does not exist.

Table 9-2 ONS 15454 Circuit States

State	Definition
IS	In service; able to carry traffic
OOS	Out of service; unable to carry traffic
OOS-AINS	Out of service, auto in service; traffic is carried, but alarms are suppressed and loopbacks are allowed. VT circuits generally switch to IS when source and destination ports are placed in IS, OOS_AINS, or OOS_MT regardless of whether a physical signal is present. STS circuits switch to IS when a signal is received.
OOS-MT	Out of service, maintenance; traffic is carried, but alarms are suppressed and loopbacks are allowed

NTP-150 Locate and View Circuits

Purpose	This procedure provides tasks that you can use to locate and view ONS 15454 circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuit creation procedure(s) in Chapter 6, "Create Circuits and VT Tunnels"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Log into the network where you want to view the circuits. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 To search for a circuit, go to the "DLP-131 Search for Circuits" task on page 9-5.

Step 3 To filter the display of circuits on the Circuits window, go to the "DLP-228 Filter the Display of Circuits" task on page 9-4.

Step 4 To view circuits on a span, go to the "DLP-229 View Circuits on a Span" task on page 9-6.

DLP-228 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the ONS 15454 network, node, or card view Circuits window based on circuit name, size, type, direction and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Switch 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, switch to node view, then double-click the card on the shelf graphic to display 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. On the Filter Dialog, set the filter attributes:

- *Name*—Enter a complete or partial circuit name to filter circuits based on 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).
- Status—Choose one: **Any** (status not used to filter circuits), **Active** (display only active circuits), **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).
- Slot—Enter a slot number to filter circuits based on source or destination slot; otherwise leave the field blank.
- *Port*—Enter a port number to filter circuits based on 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), or **VT Tunnel** (displays only VT tunnels).
- *Size*—Click the appropriate checkboxes to filter circuits based on size: VT1.5, STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, STS-192c. The checkboxes displayed depend on the entry in *Type*. 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, only STS-1 is available.

Step 4 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box are displayed 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-131 Search for Circuits

Purpose	Use this task to search for an ONS 15454 circuit at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Switch 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, switch to node view, then double-click the card on the shelf graphic to display 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 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 box to instruct CTC to select circuits only if the entire word matches the text in the *Find What* field.
- *Match Case*—Check this 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 5–6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-229 View Circuits on a Span

Purpose	View circuits on an ONS 15454 span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span. See Chapter 6, "Create Circuits and VT Tunnels" DLP-60 Log into CTC, page 3-22
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**.

Step 2 Place your mouse cursor directly over the span (green line) containing the circuits you want to view, press the right mouse button, and choose one of the following:

- **Circuits**—To view BLSR, UPSR, 1+1, or unprotected circuits on the span.
- **PCA Circuits**—To view circuits routed on a BLSR protected channel. (This option does not display if the span you right-clicked is not a BLSR span.)

On the Circuits on Span dialog box, you can view the following information for circuits provisioned on the span:

- *STS*—STSs used by the circuits.
- *VT*—VTs used by the circuits (VT circuits).
- *UPSR*—(UPSR span only)—Is checked for UPSR circuits.
- *Circuit*—Displays the circuit name.
- *Switch State*—(UPSR span only) Displays the switch state of the circuit, that is, whether any span switches are active. For UPSR 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 UPSR, you can switch the span traffic. See "DLP-94 UPSR Protection Switching Test" task on page 5-35 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-231 Edit a Circuit Name" task on page 9-8 or the "DLP-233 Edit UPSR Circuit Path Selectors" task on page 9-10 for instructions.

Step 3 Return to your originating procedure (NTP).

NTP-151 Modify Circuit Characteristics

Purpose	This procedure provides tasks that you can use to edit or change the properties of ONS 15454 circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "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 Log into the network containing the circuit you want to modify. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 To edit a circuit name, go to the "DLP-231 Edit a Circuit Name" task on page 9-8.

Step 3 To change the active and standby span colors of circuits displayed on the Edit Circuit window, go to the "DLP-232 Change Active and Standby Span Color" task on page 9-9.

Step 4 To edit a UPSR circuit, go to the "DLP-233 Edit UPSR Circuit Path Selectors" task on page 9-10.

DLP-230 Change a Circuit State

Purpose	Use this task to change the state of a circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit with the state 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 3 From the Tools menu, choose **Circuits > Set Circuit State**.

Note Alternatively, you can click the **Edit** button, then click the **State** tab on the Edit Circuits window.

Step 4 On the Set Circuit State dialog box (Figure 9-2) change the circuit state by choosing one of the following from the Target Circuit State drop-down menu:

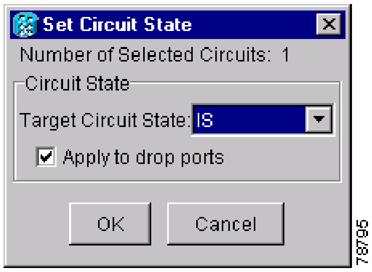
- *IS*--Places the circuit in service

- *OOS*—Places the circuit out of service
- *OOS-AINS*—The circuit is placed in out of service, auto in service
- *OOS-MT*—The circuit is placed in out of service, maintenance.

See Table 9-2 on page 9-3 for additional information about circuit states.

Step 5 If you want to apply the state to the circuit source and destination ports, check the **Apply to Drop Ports** checkbox.

Figure 9-2 Changing circuit state


Set Circuit State

Number of Selected Circuits: 1

Circuit State

Target Circuit State: IS

☑ Apply to drop ports

Step 6 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 and you change state from IS to an OOS state. If this occurs, a message is displayed and you will need to change the port state manually.

Step 7 Return to your originating procedure (NTP).

DLP-231 Edit a Circuit Name

Purpose	Use this task to edit a circuit name.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit you want to rename, then click **Edit** (or you can double-click the circuit).

Step 3 On the General tab, click the *Name* field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters. However, if you will ever 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 4 Click the **Apply** button.

Step 5 From File menu, select **Close**.

Step 6 On the Circuits window, verify that the circuit was correctly renamed.

Step 7 Return to your originating procedure (NTP).

DLP-232 Change Active and Standby Span Color

Purpose	Use this task to change the color of active (working) and standby (protect) circuit spans displayed on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 On the Preferences dialog box, click the **Circuits** 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 Change the color of the active span:

a. Next to Active Span Color, click the **Color** button.

b. On the Pick a Color dialog box, click the color for the active span, or click the **Reset** button 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 displayed.

Step 5 Change the color of the standby span:

a. Next to Standby Span Color, click the **Color** button.

b. On the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button 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 displayed.

Step 6 If you want to return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. On the Preferences dialog box, click the **Circuits** tab.

c. Click the **Reset to Defaults** button.

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 displayed.

Step 7 Return to your originating procedure (NTP).

DLP-233 Edit UPSR Circuit Path Selectors

Purpose	Use this task to change the UPSR signal fail and signal degrade thresholds, the reversion time and PDI-P settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-44 Provision UPSR Nodes, page 5-31 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 On the Circuits tab, click the UPSR circuit you want to edit.

Step 3 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

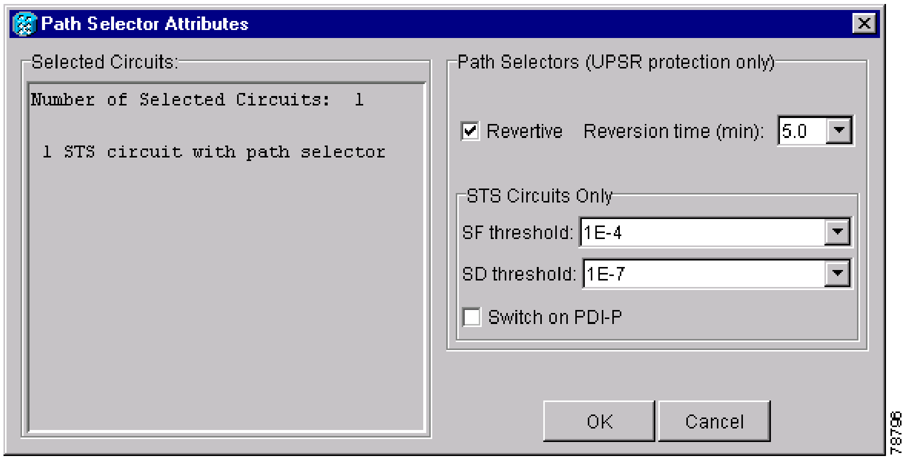
Note Alternatively, you can click the **Edit** button, then click the **UPSR Selectors** tab on the Edit Circuits window.

Step 4 On the Path Selectors Attributes dialog box (Figure 9-3), edit the following UPSR selectors, as needed:

- *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 UPSR signal failure BER threshold (STS circuits only).
- *SD Ber Level*—Sets the UPSR signal degrade BER threshold (STS circuits only).
- *PDI-P*—When checked, traffic switches if an STS payload defect indication is received (STS circuits only).

Step 5 Click **Apply**, then check that the selector switches are displayed as you expect.

Figure 9-3 Editing UPSR path selectors



Number of Selected Circuits: 1

1 STS circuit with path selector

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

☐ Switch on PDI-P

Step 6 Return to your originating procedure (NTP).

NTP-152 Delete Circuits

Purpose	Use this task to delete circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 6, "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 Log into an ONS 15454 node on the network where you want to delete the circuit. See the DLP-60 Log into CTC, page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7 for instructions.

Step 3 Investigate all network alarms and resolve any problems that may be affected by the circuit deletion. Refer to the Alarm Troubleshooting chapter in the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Verify that traffic is no longer carried on the circuit, and the circuit can be safely deleted.

Step 5 Click the **Circuits** tab.

Step 6 Choose the circuit you want to delete, then click **Delete**.

Step 7 On the Delete Circuits confirmation dialog box, check **Set** drop ports to OOS, if allowed if you want to put the circuit source and destination ports out of service. (CTC will place the ports out of service only if the circuit is in full control of the port.) Click **Yes** to confirm the deletion.

Step 8 Perform a database backup. See the "NTP-108 Back Up the Database" procedure on page 15-7 for instructions.

NTP-78 Create a Monitor Circuit

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.

Purpose	Use this task to create a monitor circuit that monitors traffic on primary, bidirectional circuits.
Tools/Equipment	None
Prerequisite Procedures	Bidirectional (2-way) circuits must exist on the network. See Chapter 6, "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 Log into an ONS 15454 node on the network where you will create the monitor circuit. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Choose the bidirectional (2-way) circuit that you want to monitor and click **Edit**.

Step 5 Verify that the circuit name is no more 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 On the Edit Circuit dialog box, click the **Monitors** tab.

The Monitors tab displays ports that you can use to monitor the circuit selected in Step 4.

Note The Monitor tab is only available when the circuit is in Active state.

Step 7 On the Monitors tab, choose a port. The monitor circuit displays traffic coming into the node at the card/port you choose.

Note In Figure 9-4, 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 On the Circuit Creation dialog box, choose the destination node, slot, port, STS, VT or DS1 for the monitored circuit.

Note In the Figure 9-4 example, this is Port 2 on the EC1-12 card.

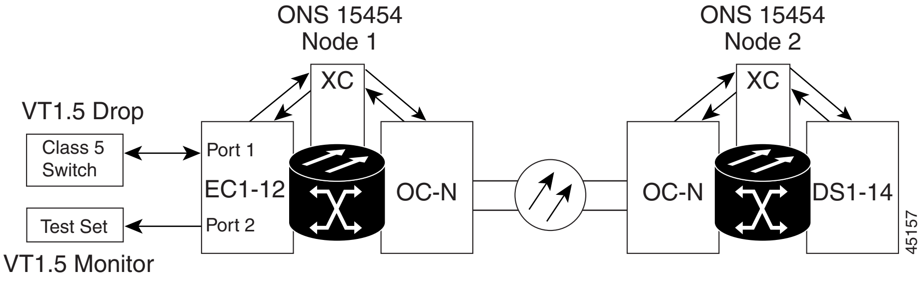
Step 10 Click **Next**.

Step 11 On the confirmation dialog box, review the monitor circuit information. Click **Finish**.

Step 12 On the Edit Circuit dialog box, click **Close**. The new monitor circuit displays on the Circuits tab.

Figure 9-4 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 procedure assumes circuits have been created.

Figure 9-4 A VT1.5 monitor circuit received at an EC1-12 port



NTP-79 Create a J1 Path Trace

Purpose	Use this procedure to create a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic.
Tools/Equipment	ONS 15454 cards capable of transmitting and/or receiving path trace must be installed. See Table 9-3 on page 9-14 for a list of cards.
Prerequisite Procedures	Path trace can only be provisioned on OC-N (STS) circuits. See Chapter 6, "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

Step 1 Log into the node on the network where you will create the path trace. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Complete the following tasks as needed:

- To create a path trace at the circuit source and destination ports, complete the "DLP-136 Provision Path Trace on Circuit Source and Destination Ports" task on page 9-14.
- To create a path trace at the OC-N ports on the circuit route, complete the "DLP-137 Provision Path Trace on OC-N Ports" task on page 9-18.

DLP-136 Provision Path Trace on Circuit Source and Destination Ports

Purpose	Use this task to create a path trace on an STS circuit source and destination ports.
Tools/Equipment	ONS 15454 cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 9-3 on page 9-14 for a list of cards.
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure assumes you are setting up path trace on a bidirectional circuit, and you will set transmit strings at the circuit source and destination.

Step 1 Click the **Circuits tab**.

Step 2 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 9-3 for a list of cards.

Table 9-3 ONS 15454 Cards Capable of Path Trace

J1 Function	Cards
Transmit and Receive	DS1-14, DS1N-14, DS3-12E, DS3N-12E, DS3XM-6, G1000-4
Receive Only	EC1-12 OC3 IR 4 1310 OC12/STM4-4 OC48 IR/STM16 SH AS 1310, OC48 LR/STM16 LH AS 1550 OC192 LR/STM64 LH 1550

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 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.

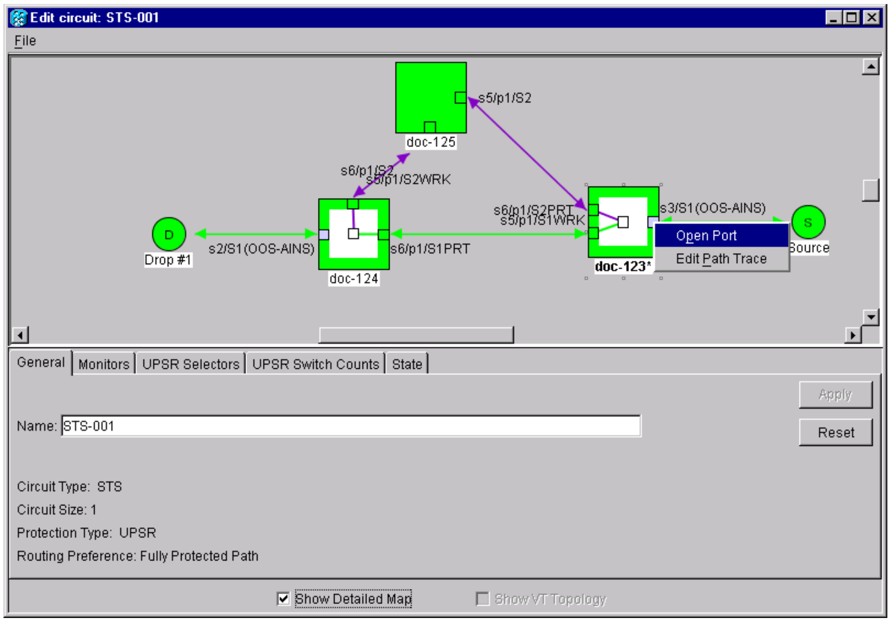
Step 3 Choose the STS circuit you want to trace, then click **Edit**.

Step 4 On the Edit Circuit window, click the *Show Detailed Map* box at the bottom of the window. A detailed map of the source and destination ports is displayed.

Step 5 Provision the circuit source transmit string:

a. On the detailed circuit map right-click the circuit source port (square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu. Figure 9-5 shows an example.

Figure 9-5 Selecting the Edit Path Trace option



Name: STS-001

Circuit Type: STS
Circuit Size: 1
Protection Type: UPSR
Routing Preference: Fully Protected Path

☑ Show Detailed Map ☐ Show VT Topology

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 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 6 Provision the circuit destination transmit string:

a. On the Edit Circuit window (with Show Detailed Map chosen, see Figure 9-5) right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu.

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 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 7 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 the baseline. An alarm is raised when a string that differs from the baseline is received.
- *Manual*—the string entered in *Current Expected String* is the baseline. An alarm is raised when a string that differs from the *Current Expected String* is received.

b. If you set *Path Trace Mode* 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 on TIM-P** checkbox if you want to suppress the Alarm Indication Signal when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

Note RDI (Remote Defect Indicator) conditions on TIM-P are not generated in this release.

d. Click **Apply**, then click **Close.**

Step 8 Provision the circuit source expected string:

a. On the Edit Circuit window (with Show Detailed Map chosen, see Figure 9-5) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. 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*—Uses the first string received from port at the other 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 *Path Trace Mode* 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 on TIM-P** checkbox if you want to suppress the Alarm Indication Signal when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

e. Click **Apply.**

Step 9 After you set up the path trace, the received string is displayed in the Received box on the path trace setup window. Figure 9-6 shows an example. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal display. The button name changes to ASCII Mode. Click it to return the path trace to ASCII display.
- 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).

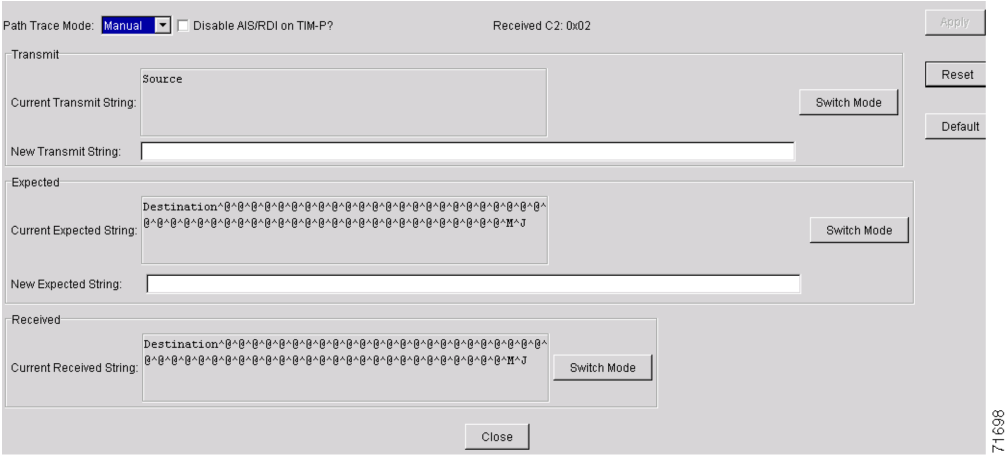
Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The Expect and Receive strings are updated every few seconds as long as *Path Trace Mode* is set to Auto or Manual.

Step 10 Click **Close.**

When you display the detailed circuit window, path trace is indicated by an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports. Figure 9-7 shows an example.

Figure 9-6 Setting up a path trace



Path Trace Mode: Manual
□ Disable AIS/RDI on TIM-P?
Received C2: 0x02

Transmit

Current Transmit String:

```
Source
```

New Transmit String:

Expected

Current Expected String:

```
Destination^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^M^J
```

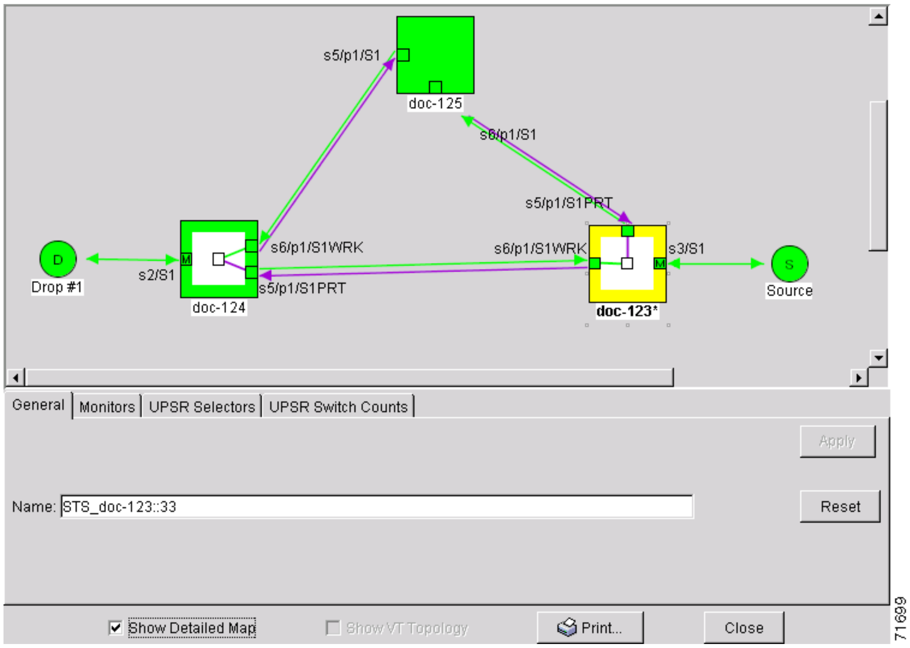
New Expected String:

Received

Current Received String:

```
Destination^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^M^J
```

Figure 9-7 Detailed circuit window with Manual expected string enabled



Name: STS_doc-123::33

Step 11 Return to your originating procedure (NTP).

DLP-137 Provision Path Trace on OC-N Ports

Purpose	Use this task to monitor a path trace on OC-N ports within the circuit path.
Tools/Equipment	ONS 15454 cards capable of receiving path trace must be installed at the OC-N circuit ports. See Table 9-3 on page 9-14.
Prerequisite Procedures	DLP-136 Provision Path Trace on Circuit Source and Destination Ports, page 9-14.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display 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 On the Edit Circuit window, click the *Show Detailed Map* box at the bottom of the window. A detailed circuit graphic showing source and destination ports is displayed.

Step 5 On the detailed circuit map right-click the circuit OC-N port (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 9-3 on page 9-14. If not, the Edit Path Trace menu item will not display.

Step 6 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*—Uses the first string received from port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended, since 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 *Path Trace Mode* 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 *Path Trace Mode* to Auto, skip this step.

Step 8 Click the **Disable AIS on TIM-P** checkbox if you want to suppress the Alarm Indication Signal when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.

Step 9 Click **Apply**, then click **Close.**

Step 10 Return to your originating procedure (NTP).

CHAPTER 10

Change Node Settings

This chapter explains how to modify node provisioning. 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, see Appendix C, "Network Element Defaults."

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-81 Change Node Management Information, page 10-2—As needed, complete this procedure to change node name, contact information, latitude, longitude, date, and time.
2. NTP-82 Change CTC Network Access, page 10-4—As needed, complete these procedures to change the IP address, default router, subnet mask, and network configuration settings, and to modify static routes.
3. NTP-83 Customize the CTC Network View, page 10-9—As needed, complete this procedure to customize the appearance of the network map, including specifying a different default map, selecting your own map or image, and changing the background color.
4. NTP-84 Modify or Delete Card Protection Settings, page 10-14—As needed, complete these procedures to modify and delete 1:1, 1:N, and 1+1 protection groups.
5. NTP-85 Change Node Timing, page 10-20—As needed, complete these procedures to make changes to the network timing parameters.
6. NTP-86 Modify Users and Change Security, page 10-22—As needed, complete these procedures to make changes to user settings and to delete users.
7. NTP-87 Change SNMP Settings, page 10-26—As needed, complete these procedures to modify or delete SNMP.

NTP-81 Change Node Management Information

Purpose	Use this procedure to change basic information about the node to facilitate node management.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22. If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Return to node view and click the **Provisioning > General** tabs.

Step 4 As needed, complete the "DLP-140 Change the Node Name, Date, Time, and Contact Information" task on page 10-2.

Note Changing the date, time, or time zone may invalidate the node's performance monitoring counters.

Step 5 As needed, complete the "DLP-265 Change the Login Legal Disclaimer" task on page 10-3.

Step 6 When the changes appear, complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-140 Change the Node Name, Date, Time, and Contact Information

Purpose	Use this procedure to change basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- Node Name
- Contact
- Location: Latitude
- Location: Longitude

- Location: Description

Note To see changes to longitude or latitude reflected on the network map, you must go to network view and right-click on the specified node, then click Reset Node Position.

- Use SNTP Server
- Date
- Time
- Time Zone
- Use Daylight Saving Time

  See the "NTP-26 Set Up CTC Network Access" procedure on page 4-5 for detailed field descriptions.

Note Changing the date, time, or time zone may invalidate the node's performance monitoring counters.

Step 3 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task and refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Return to the "NTP-81 Change Node Management Information" procedure on page 10-2.

DLP-265 Change the Login Legal Disclaimer

Purpose	Use this procedure to modify 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-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser or higher

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. You can also use the following HTML commands to format the text:

- <b> Begins boldface font
- </b> 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
- </font> 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 the "NTP-81 Change Node Management Information" procedure on page 10-2.

NTP-82 Change CTC Network Access

The following procedures explains how to change essential ONS 15454 networking information. 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*.

Purpose	Use this procedure to change essential network information, including IP settings, static routes, and OSPF options.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22. If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-141 Change IP Address, Subnet Mask, Default Router, and Network Defaults, page 10-5
- DLP-142 Modify a Static Route, page 10-6
- DLP-143 Delete a Static Route, page 10-7
- DLP-144 Disable OSPF, page 10-8

- DLP-66 Set Up or Change Open Shortest Path First Protocol, page 4-12 to change any OSPF settings.

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-141 Change IP Address, Subnet Mask, Default Router, and Network Defaults

Purpose	Use this task to change the IP address, subnet mask, default router, and network defaults for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Network** tabs (Figure 10-1).

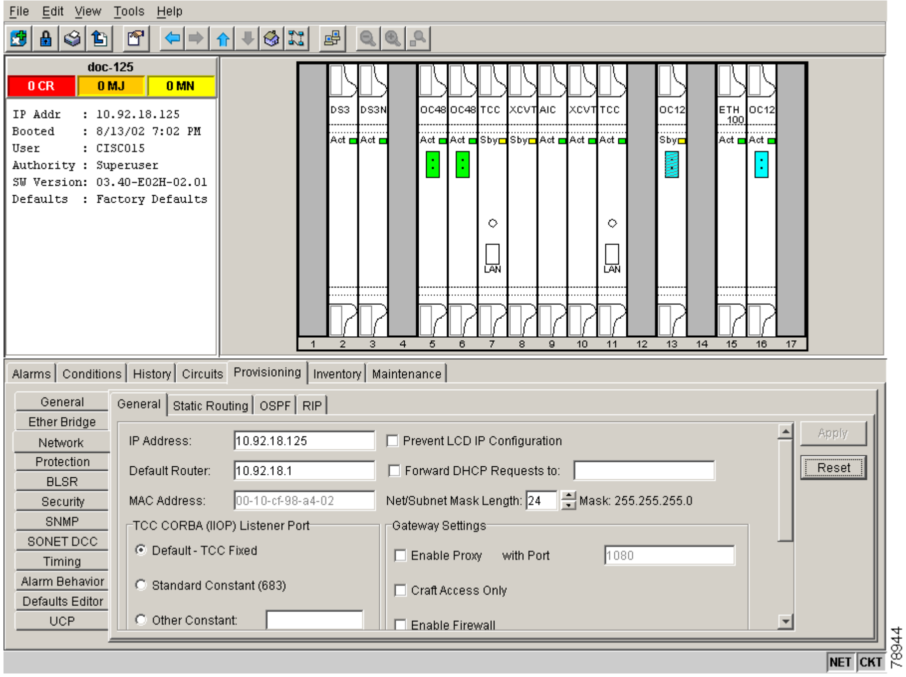
Step 2 Change any of the following:

- *IP Address*
- *Prevent LCD IP Config*
- *Default Router*
- *Subnet Mask Length*
- *Forward DHCP Request To*
- *TCC CORBA (IIOP) Listener Port*
- *Gateway Settings*

See the "DLP-64 Set the IP Address, Default Router, and Network Mask Using the LCD" task on page 4-9 for detailed field descriptions.

Note Modifying the IP address, default router, subnet mask length, or TCC CORBA (IIOP) Listener Port will cause the TCCs to reboot. This results in a temporary loss of connectivity to the node, but traffic is unaffected.

Figure 10-1 Changing general network information



```
IP Addr    : 10.92.18.125
Booted     : 8/13/02 7:02 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.40-E02H-02.01
Defaults   : Factory Defaults
```

IP Address: 10.92.18.125

Default Router: 10.92.18.1

MAC Address: 00-10-cf-98-a4-02

□ Prevent LCD IP Configuration

□ Forward DHCP Requests to:

Net/Subnet Mask Length: 24 Mask: 255.255.255.0

TCC CORBA (IIOP) Listener Port

● Default - TCC Fixed

○ Standard Constant (683)

○ Other Constant:

Gateway Settings

□ Enable Proxy with Port 1080

□ Craft Access Only

□ Enable Firewall

Step 3 Click **Apply**.

Step 4 Click **Yes** on the Change Network Configuration? dialog box.

Both ONS 15454 TCC+ cards will reboot, one at a time. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-142 Modify a Static Route

Purpose	Use this task to modify a static route on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node (default) 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 (see the "DLP-65 Create a Static Route" task on page 4-11 for detailed field descriptions):

- *Mask*
- *Next Hop*
- *Cost*

Step 6 Click **OK**.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 7 Return to your originating procedure (NTP).

DLP-143 Delete a Static Route

Purpose	Use this task to delete an existing static route on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 Routing** tab.

Step 3 Click the static route you want to delete.

Step 4 Click **Delete**. A confirmation dialog box appears.

Step 5 Click **Yes** to confirm deletion of the static route.

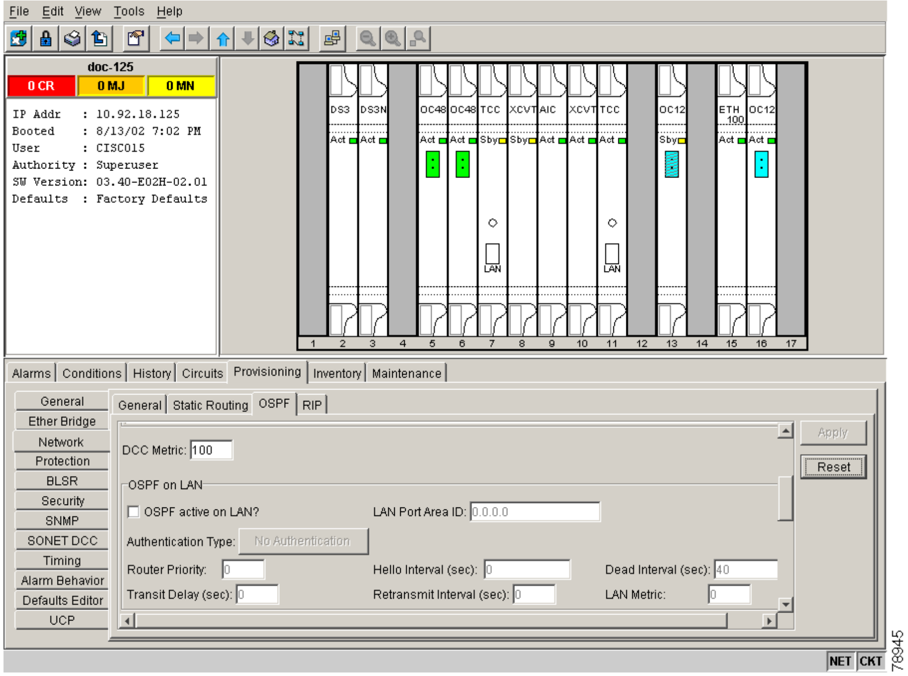
Step 6 Return to your originating procedure (NTP).

DLP-144 Disable OSPF

Purpose	Use this task to disable the Open Shortest Path First (OSPF) routing protocol process for the LAN on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, select the **Provisioning** > **Network** > **OSPF** tabs (Figure 10-2). The OSPF subtab has several options.

Figure 10-2 Disabling OSPF on the ONS 15454



doc-125
0 CR 0 MJ 0 MN

```
IP Addr   : 10.92.18.125
Booted    : 8/13/02 7:02 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

DCC Metric: 100

OSPF on LAN

☐ OSPF active on LAN?

LAN Port Area ID: 0.0.0.0

Authentication Type: No Authentication

Router Priority: 0

Hello Interval (sec): 0

Dead Interval (sec): 40

Transit Delay (sec): 0

Retransmit Interval (sec): 0

LAN Metric: 0

File Edit View Tools Help
DS3 DS3N OC48 OC48 TCC XCVT AIC XCVT TCC OC12 ETH 100 OC12
Act Act Act Act Sby Sby Act Act Act Sby Act Act
LAN
LAN
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Alarms Conditions History Circuits Provisioning Inventory Maintenance
General
Ether Bridge
Network
Protection
BLSR
Security
SNMP
SONET DCC
Timing
Alarm Behavior
Defaults Editor
UCP
General Static Routing OSPF RIP
Apply
Reset
NET CKT
78945

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN** checkbox.

Note If you disable OSPF, the DCC OSPF area ID appears as 192.168.190.0.

Step 3 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Return to your originating procedure (NTP).

Note Disabling OSPF can cause the TCCs to reboot. This results in a temporary loss of connectivity to the node, but traffic is unaffected.

NTP-83 Customize the CTC Network View

Purpose	Use this procedure to modify 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 Log into an ONS 15454. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Complete the following tasks, as needed:

- DLP-145 Change the Network View Background Color, page 10-9
- DLP-146 Change the Default Network View Map, page 10-10
- DLP-147 Apply a Custom Network View Background Map, page 10-11
- DLP-148 Create Domain Icons, page 10-12
- DLP-149 Manage Domain Icons, page 10-13

DLP-145 Change the Network View Background Color

Purpose	Use this task to change the network view background color and the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning 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 If CTC is in card or node view, from the View menu, select **Go to Network View**.

Step 2 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 3 On the Choose Color dialog box, select a background color.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-146 Change the Default Network View Map

Purpose	Use this task to change the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If CTC is in card or node view, from the View menu, choose **Go to Network View**.

Step 2 From the Edit menu, choose **Preferences**.

Step 3 On the **Map** tab of the Preferences dialog box, click the Default Maps field and choose a default map from the pull-down menu. The default map choices include Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 4 Click **Apply**. The new default network map is displayed.

Step 5 Click **OK**.

Step 6 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until the ONS 15454 icons are visible.

Step 7 Press **Ctrl**, click an ONS 15454 icon, and drag it to a new location.

Step 8 Repeat Step 7 to position each ONS 15454 icon.

Step 9 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-147 Apply a Custom Network View Background Map

Purpose	Use this task to change the background image or map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

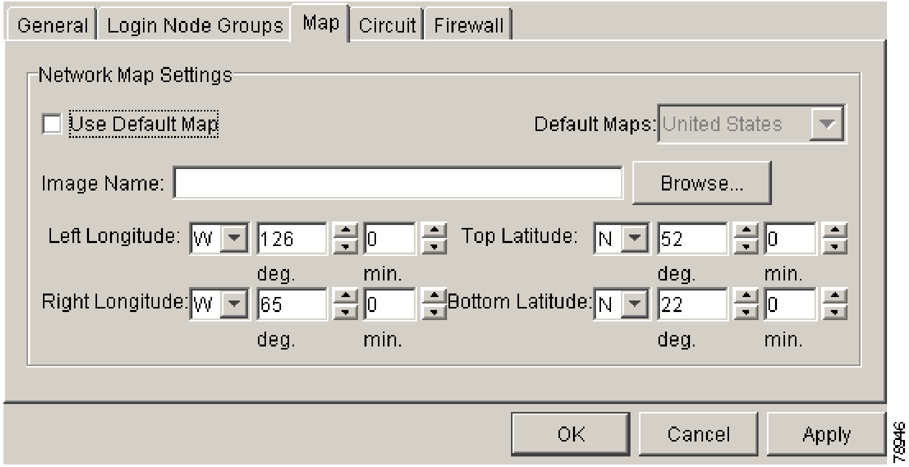
Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you want to position nodes on the map based on the node coordinates, you will need the longitudes and latitudes for the edges of the map. You can obtain the longitude and latitude for cities and Zip Codes from the U.S. Census Bureau U.S. Gazetteer website (www.census.gov/cgi-bin/gazetteer). If you will use your mouse to position nodes, coordinates for the image edges are not necessary. The change does not affect other CTC users.

Step 1 If CTC is in card or node view, from the View menu, choose **Go to Network View**.

Step 2 From the Edit menu, choose **Preferences**. (You also right-click the network or domain map and select **Set Background Image**.)

Step 3 On the **Map** tab of the Preferences dialog box (Figure 10-3), deselect **Use Default Map**.

Figure 10-3 Changing the CTC background image



Network Map Settings

☐ Use Default Map

Default Maps: United States

Image Name:

Left Longitude: W 126 deg. 0 min.

Top Latitude: N 52 deg. 0 min.

Right Longitude: W 65 deg. 0 min.

Bottom Latitude: N 22 deg. 0 min.

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 (Optional) Enter the coordinates for the map image edges in the longitude and latitude fields on the Preferences dialog box. CTC uses the map's longitude and latitude to position the node icons based on the node coordinates entered for each node on the Provisioning > General tabs. Coordinates only need to be precise enough to place ONS node icons in approximate positions on the image.

Tip You can also drag and drop nodes to position them on the network view map.

Step 7 Click **Apply** and then click **OK**.

Step 8 If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until the ONS 15454 icons are visible.

Step 9 Press **Ctrl**, click an ONS 15454 icon, and drag it to a new location.

Step 10 Repeat Step 9 until all ONS 15454 icons are positioned where you want them.

Step 11 Right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.

Step 12 At the network view, use the CTC toolbar Zoom buttons (or right-click the graphic area and select a Zoom command from the shortcut menu) to set the area of the image you can view.

Step 13 Return to your originating procedure (NTP).

DLP-148 Create Domain Icons

Purpose	Use this task to create a domain icon, which can be used to group ONS 15454 icons in CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Domains you create will be seen by all users who log into the network.

Step 1 If CTC is in card or node view, 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-149 Manage Domain Icons

Purpose	Use this task to manage CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-60 Log into CTC, page 3-22 DLP-148 Create Domain Icons, page 10-12
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain actions, such as adding or removing node icons, will be seen by all users who log into the network.

Step 1 If CTC is in card or node view, from the View menu, choose **Go to Network View**.

Step 2 Locate the domain action you want in Table 10-1 and complete the appropriate steps.

Table 10-1 Managing Domains

Domain action	Steps
Move a domain	Pressing **Ctrl**, drag 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 a node icon to the domain icon. Release the mouse button when the node icon is over the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Select **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 residing in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

NTP-84 Modify or Delete Card Protection Settings

Purpose	Use this procedure to modify or delete card protection settings.
Tools/Equipment	None
Prerequisite Procedures	None
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 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22. If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Display the node (default) view. Perform any of the following tasks as needed:

- DLP-150 Modify a 1:1 Protection Group, page 10-14
- DLP-152 Modify a 1:N Protection Group, page 10-16
- DLP-154 Modify a 1+1 Protection Group, page 10-17
- DLP-155 Delete a Protection Group, page 10-18

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-150 Modify a 1:1 Protection Group

Purpose	Use this task to modify a 1:1 protection group for electrical (DS-1, DS-3, EC-1, and DS3XM-6) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Protection** tabs (Figure 10-4).

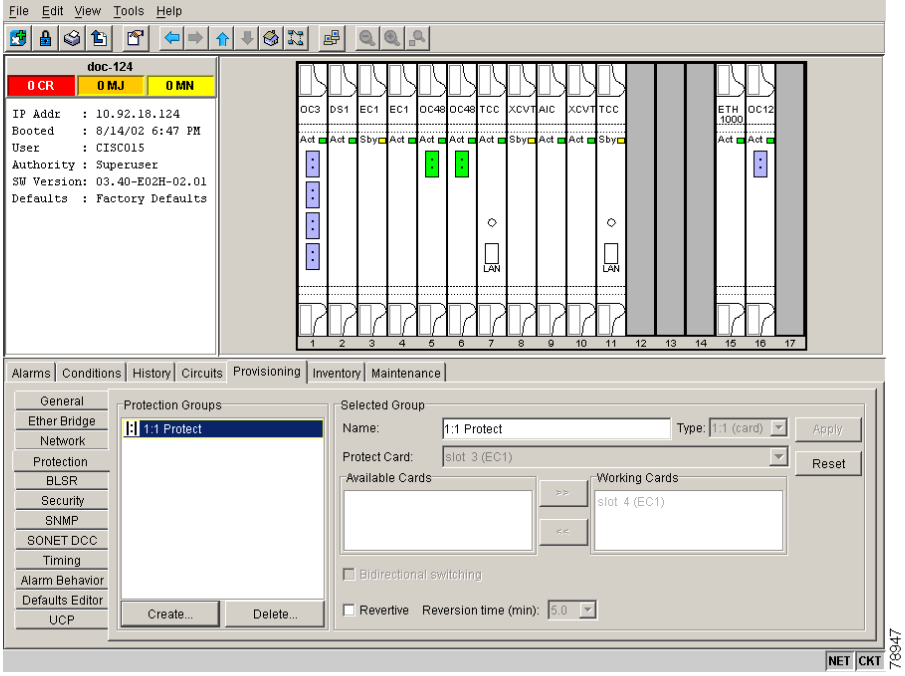
Step 2 Under Protection Groups, click the 1:1 protection group you want to modify.

Step 3 Under Selected Group, you can modify the following:

- *Name*—Type a name for the protection group. 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 entered in *Reversion Time*.

- *Reversion time*—If *Revertive* is checked, choose the reversion time. Click the *Reversion time* field and select a reversion time from the pull-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.

Figure 10-4 Modifying a 1:1 protection group



```
IP Addr    : 10.92.18.124
Booted     : 8/14/02 6:47 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.40-E02H-02.01
Defaults   : Factory Defaults
```

Protection Groups: 1:1 Protect

Name: 1:1 Protect Type: 1:1 (card)

Protect Card: slot 3 (EC1)

Working Cards: slot 4 (EC1)

☐ Bidirectional switching

☐ Revertive Reversion time (min): 5.0

Step 4 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

Note To convert protection groups, see the "NTP-91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 11-33.

DLP-152 Modify a 1:N Protection Group

Purpose	Use this task to modify a 1:N protection group for DS-1 and DS-3 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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-72 Create a 1:N Protection Group" task on page 4-26.

Step 2 From node view, click the **Provisioning** > **Protection** tabs (Figure 10-5).

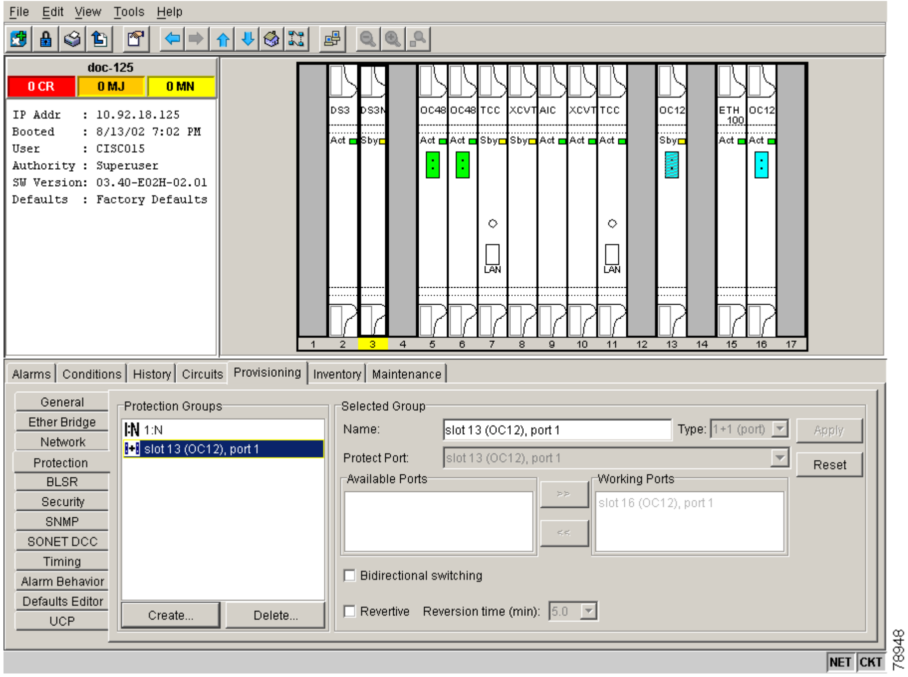
Step 3 Under Protection Groups, click the 1:N protection group you want to modify.

Step 4 Under Selected Group, enter the following:

- *Name*
- *Available Cards*
- *Working Cards*
- *Reversion Time*

See the "DLP-72 Create a 1:N Protection Group" task on page 4-26 for field descriptions.

Figure 10-5 Modifying a 1:N protection group



```
IP Addr   : 10.92.18.125
Booted    : 8/13/02 7:02 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Protection Groups
1:N
slot 13 (OC12), port 1

Selected Group
Name: slot 13 (OC12), port 1
Type: 1+1 (port)
Protect Port: slot 13 (OC12), port 1
Available Ports
Working Ports: slot 16 (OC12), port 1
□ Bidirectional switching
□ Revertive Reversion time (min): 5.0

Step 5 Click **Apply**. The changes are applied. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Return to your originating procedure (NTP).

Note To convert protection groups, see the "NTP-91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 11-33.

DLP-154 Modify a 1+1 Protection Group

Purpose	Use this task to modify a 1+1 protection group for any optical port (OC-3, OC-12, OC-48, OC-48AS, OC-192, and OC-12 IR)
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Protection** tabs (Figure 10-6).

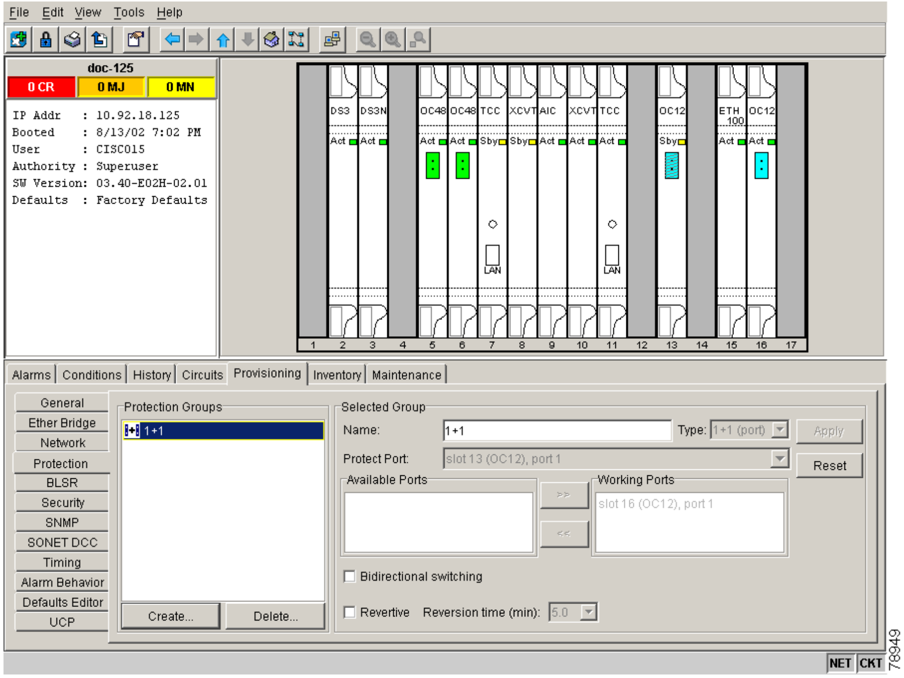
Step 2 Under Protection Groups, click the 1+1 protection group you want to modify.

Step 3 Under Selected Group, you can modify the following:

- *Name*
- *Bidirectional switching*
- *Revertive*
- *Reversion time*

See the "DLP-73 Create a 1+1 Protection Group" task on page 4-27 for field descriptions.

Figure 10-6 Modifying a 1+1 protection group



```
doc-125
0 CR    0 MJ    0 MN

IP Addr    : 10.92.18.125
Booted     : 8/13/02 7:02 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.40-E02H-02.01
Defaults   : Factory Defaults
```

Protection Groups: 1+1

Selected Group

Name: 1+1 Type: 1+1 (port)

Protect Port: slot 13 (OC12), port 1

Available Ports:

Working Ports: slot 16 (OC12), port 1

☐ Bidirectional switching

☐ Revertive Reversion time (min): 5.0

Step 4 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

Note To convert protection groups, see the "NTP-91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 11-33.

DLP-155 Delete a Protection Group

Purpose	Use this task to delete a protection group for any 1:1, 1:N, or 1+1 protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > Protection** tabs.

Step 2 Under Protection Groups, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box to confirm deletion. Confirm that the changes appear; if they do not, repeat Steps 1-- 3.

Step 5 Return to your originating procedure (NTP).

DLP-156 Delete a SONET DCC Termination or Tunnel

Purpose	Use this task to delete a SONET DCC termination or tunnel in a ring on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting a DCC termination or tunnel will cause you to lose visibility of other nodes in the network.

Step 1 From node view, click the **Provisioning > Sonet DCC** tabs.

Step 2 Click the DCC termination/tunnel to be deleted. The Delete SDCC Termination or Delete Tunnel dialog box opens.

Step 3 Check the **Set Unused Port Out of Service** box if you want to change the port state to out of service.

Step 4 Click **Yes** to confirm. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

Note The ONS 15454 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs; therefore, the Line DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 networks.

NTP-85 Change Node Timing

Purpose	Use this procedure to change the SONET timing settings 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 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22. If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 As needed, complete the "DLP-157 Change the Node Timing Source" task on page 10-20.

Step 4 If you need to change any internal timing settings, follow the "DLP-70 Set Up Internal Timing" task on page 4-22 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, see the "DLP-195 Verify Timing in a Reduced Ring" task on page 14-13.

Step 6 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-157 Change the Node Timing Source

Purpose	Use this task to change the SONET timing source for the ONS 15454
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 From node view, click the **Provisioning > Timing** tabs (Figure 10-7).

Step 2 In the General Timing section, change any of the following information:

- *Timing Mode*

Note Because mixed timing may 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-69 Set Up External or Line Timing" task on page 4-19 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.

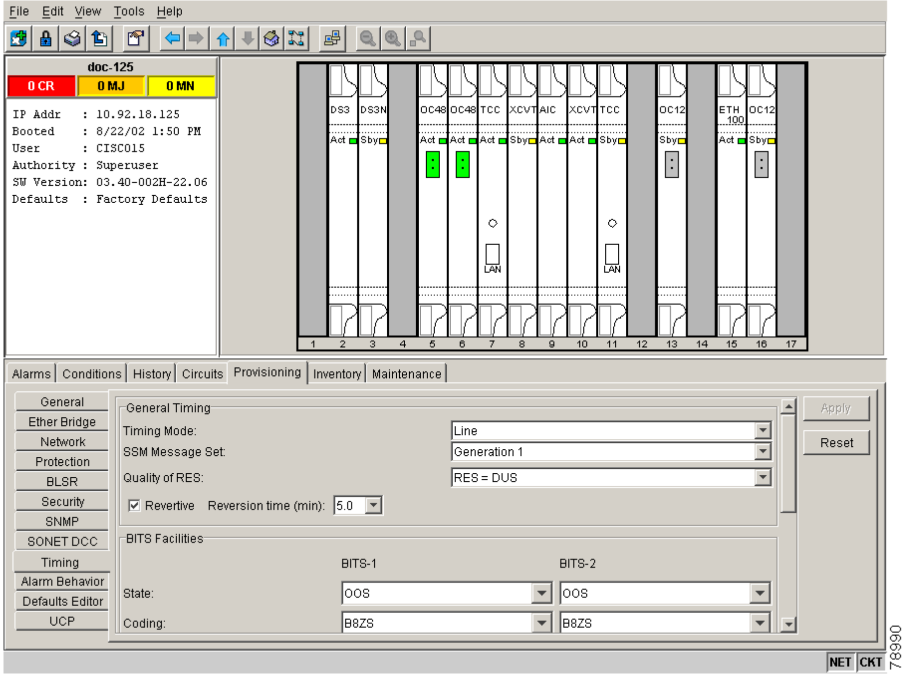
- *State*
- *Coding*
- *Framing*
- *Sync Messaging*
- *AIS Threshold*
- *LBO*

Step 4 Under Reference Lists, 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*

Figure 10-7 Modifying ONS 15454 timing



```
IP Addr   : 10.92.18.125
Booted    : 8/22/02 1:50 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-002H-22.06
Defaults  : Factory Defaults
```

General Timing

Timing Mode: Line

SSM Message Set: Generation 1

Quality of RES: RES = DUS

☑ Revertive Reversion time (min): 5.0

BITS Facilities

	BITS-1	BITS-2
State:	OOS	OOS
Coding:	B8ZS	B8ZS

Step 5 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 6 Return to your originating procedure (NTP).

Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

NTP-86 Modify Users and Change Security

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. You can perform ONS 15454 user management tasks from network or node view. In network view, you can add, edit, or delete users from multiple nodes at one time. If you perform user management tasks in node view, you can only add, edit, or delete users from that node.

See the "NTP-30 Create Users and Assign Security" procedure on page 4-28 for more information about adding users.

Purpose	Use this procedure to modify user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-158 Change User and Security Settings - Single Node, page 10-23
- DLP-159 Delete User - Single Node, page 10-24
- DLP-160 Change User and Security Settings - Multiple Nodes, page 10-24
- DLP-161 Delete User - Multiple Nodes, page 10-25

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-158 Change User and Security Settings - Single Node

Purpose	Use this task to change settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security** tabs.

Step 2 Click the user whose settings you want to modify.

Step 3 Under Selected User, you can modify the following:

- *New Password*
- *Confirm Password*
- *Security Level*

See the"NTP-30 Create Users and Assign Security" procedure on page 4-28 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

Note User settings that you changed during this task will not appear until that user logs off and logs back in again.

DLP-159 Delete User - Single Node

Purpose	Use this task to delete an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, select the **Provisioning** > **Security** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete User dialog box to confirm deletion. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-160 Change User and Security Settings - Multiple Nodes

Purpose	Use this task to modify an existing user's settings for multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed; use this procedure to add users to multiple nodes at one time
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 in node (default) view, choose **Go to Network View**. Verify that all the nodes where you want to add users are accessible in network view.

Step 2 Click the **Provisioning** > **Security** 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, enter the following:

- *New Password*
- *Confirm New Password*
- *Security Level*

See the "DLP-75 Create a New User - Multiple Nodes" task on page 4-30 for field descriptions.

Step 5 Under "Select applicable nodes," deselect any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 On the User Change Results dialog box, click **OK** to acknowledge the changes. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Return to your originating procedure (NTP).

DLP-161 Delete User - Multiple Nodes

Purpose	Use this task to delete an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To perform this task you must be assigned the superuser security level.

Step 1 From the View menu in node (default) view, 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 Under Select Applicable Nodes, deselect 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 confirm the deletion. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 7 Return to your originating procedure (NTP).

NTP-87 Change SNMP Settings

Purpose	Use this procedure to modify user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	None
Required User Level	Superuser
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To perform this procedure you must be assigned the superuser security level.

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22. If you are already logged into the correct node, proceed to Step 2.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-162 Modify SNMP Trap Destination, page 10-26
- DLP-163 Delete SNMP Trap Destination, page 10-28
- DLP-164 Delete Ethernet RMON Alarm Thresholds, page 10-29

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-162 Modify SNMP Trap Destination

Purpose	Use this task to modify SNMP settings on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Click the selected trap from **Trap Destinations** dialog box.

For a description of SNMP traps, see the *Cisco ONS 15454 Reference Guide*.

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 NMS.

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.

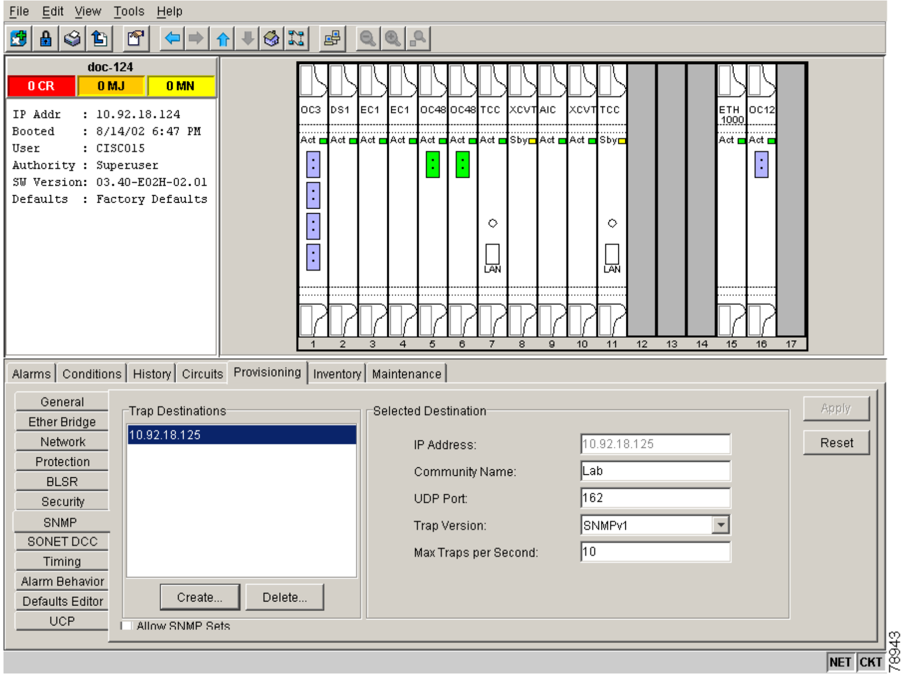
Step 6 Click **Apply**.

Step 7 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 (Figure 10-8). Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Return to your originating procedure (NTP).

Figure 10-8 Viewing trap destinations


File Edit View Tools Help
doc-124
0 CR
0 MJ
0 MN
OC3 DS1 EC1 EC1 OC48 OC48 TCC XCVT AIC XCVT TCC ETH 1000 OC12
Act Act Act Act Act Act Act Sby Act Act Sby Act Act
LAN
LAN
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Alarms Conditions History Circuits Provisioning Inventory Maintenance
General
Ether Bridge
Network
Protection
BLSR
Security
SNMP
SONET DCC
Timing
Alarm Behavior
Defaults Editor
UCP
Create...
Delete...
Apply
Reset
NET CKT
78943

```
IP Addr   : 10.92.18.124
Booted    : 8/14/02 6:47 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Trap Destinations

10.92.18.125

☐ Allow SNMP Sets

Selected Destination

IP Address:	10.92.18.125
Community Name:	Lab
UDP Port:	162
Trap Version:	SNMPv1
Max Traps per Second:	10

DLP-163 Delete SNMP Trap Destination

Purpose	Use this task to delete SNMP on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Click **the selected trap to delete from Trap Destination pane**.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes** to confirm deletion of that trap. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-164 Delete Ethernet RMON Alarm Thresholds

Purpose	This procedure deletes remote monitoring (RMON) of Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the CTC node view.

Step 2 Click the **Provisioning** > **Ether Bridge > 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

Change Card Settings

This chapter explains how to change transmission settings on cards in a Cisco ONS 15454.

Before You Begin

Before performing any of the following procedures, complete the "NTP-80 Document Existing Provisioning" procedure on page 7-2.

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-88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards, page 11-2—As needed, complete this procedure to change transmission settings, including line (drop) and threshold settings, for the electrical cards (EC-1, DS-1, DS-3, and DS3MX-6).
2. NTP-89 Modify Line Settings and PM ParameterThresholds for Optical Cards, page 11-19—As needed, complete this procedure to change transmission settings, including line (drop) and threshold settings, for all optical (OC-N) cards.
3. NTP-90 Modify Alarm Interface Controller Settings, page 11-25—As needed, complete this procedure to change external alarms and controls and/or orderwire settings.
4. NTP-118 Modify Alarm Interface Controller-International Settings, page 11-29—As needed, complete this procedure to change external alarms and controls and/or orderwire settings.
5. NTP-91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection, page 11-33—As needed, complete this procedure to change the type of protection on DS-1 and DS-3 cards.

NTP-88 Modify Line Settings and PM Parameter Thresholds for Electrical Cards

Purpose	Use this procedure to change the line and threshold settings for electrical cards; the default values are listed in the "Card Default Settings" section on page C-4.
Tools/Equipment	None
Prerequisite Procedures	NTP-23 Log into the ONS 15454 GUI, page 3-21.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Perform a database backup to preserve the existing database. See the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-165 Change Line and Threshold Settings for the DS-1 Card, page 11-2
- DLP-166 Change Line and Threshold Settings for the DS-3 Card, page 11-6
- DLP-167 Change Line and Threshold Settings for the DS3E Card, page 11-9
- DLP-168 Change Line and Threshold Settings for the DS3XM-6 Card, page 11-12
- DLP-169 Change Line and Threshold Settings for the EC-1 Card, page 11-16

Step 4 When you are finished changing the card settings, complete the "NTP-108 Back Up the Database" procedure on page 15-7.

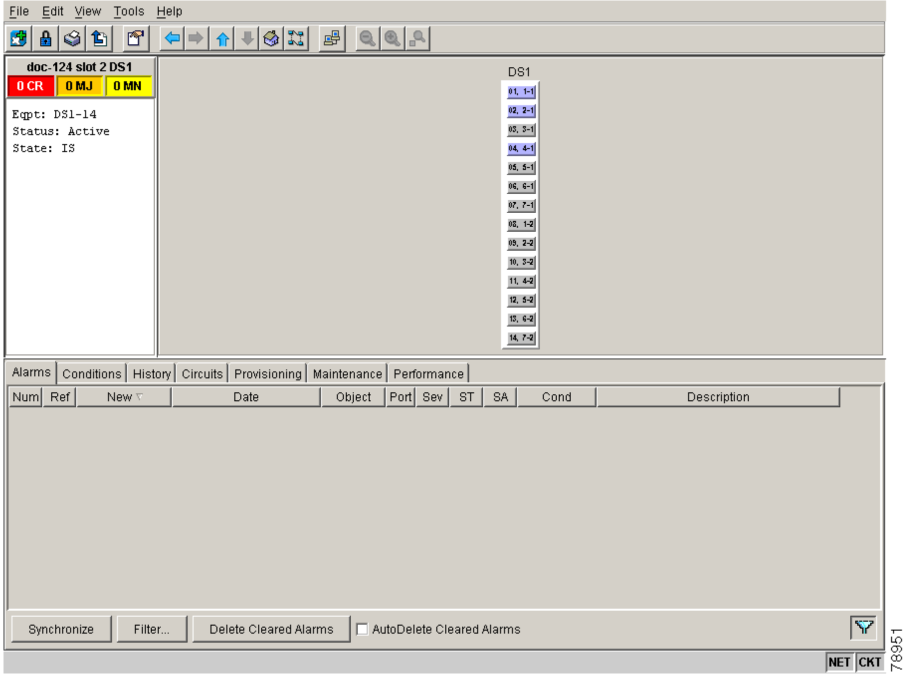
DLP-165 Change Line and Threshold Settings for the DS-1 Card

Purpose	Use this task to change the line and threshold settings for the DS-1 card. The default DS-1 card settings are listed in Table C-1 on page C-6.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

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 (Figure 11-1).

Figure 11-1 Provisioning line parameters on the DS1-14 card



```
Eqpt: DS1-14
Status: Active
State: IS
```

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, **Elect Path Thrshld**, or **Sonet Thrshld** tab.

Note See Chapter 7, "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 11-1. For definitions of the Line Threshold settings, see Table 11-2. For definitions of the Electrical Path settings, see Table 11-3.

For the factory default settings for the DS1-14 and DS1-14N Cards, see Table C-1 on page C-6.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

Step 7 Return to your originating procedure (NTP).

Table 11-1 Line Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port #	Port number	1 - 14 (read-only)
Port	Port name	User-defined, up to 32 alphanumeric/special characters. Blank by default To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
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 backplane connection to the next termination point	• 0 - 131 • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
State	Places port in or out of service	See the "DLP-214 Change the Service State for a Port" task on page 5-5
AINS Soak	Automatic in-service soak	• Time of presence of valid input signal in hh.mm after which the card is set in service by the software. • 0 to 48 hours, 15 minutes increments.

Table 11-2 Line Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port	Port number	1 - 14 (read-only)
CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
LOSS	Number of one-second intervals containing one or more loss of signal defects	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-3 Electrical Path Threshold Options for DS1-14 and DS1N-14 Cards

Parameter	Description	Options
Port	Port number	1 - 14 (read-only)
CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
SAS	Severely errored frame/alarm indication signal	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
AISS	Alarm indication signal seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-4 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 bullet and click Show Threshold button (Near End, STS termination).
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near End, STS termination).
FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near End, STS termination).

Table 11-4 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 bullet and click Show Threshold button (Near End, STS termination).
UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near End, STS termination).

Note The threshold value will be displayed after the circuit is created.

DLP-166 Change Line and Threshold Settings for the DS-3 Card

Purpose	Use this task to change the line and threshold settings for the DS-3 card. The default DS-3 values are listed in Table C-2 on page C-7.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

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 Thrshld**, **Elec Path Thrshld**, or **Sonet Thrshld** subtab.

Note See Chapter 7, "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 11-5. For definitions of the Line Threshold settings, see Table 11-6. For definitions of the SONET Threshold settings, see Table 11-7.

For the factory default settings for the DS3-12 and DS3N-12 Cards, see Table C-2 on page C-7.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

Step 7 Return to your originating procedure (NTP).

Table 11-5 Line Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port #	Port number	1 - 12
Port	Port name	User-defined, up to 32 alphanumeric/ special characters. Blank by default. To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 225 (default) • 226 - 450
State	Places port in or out of service	See the "DLP-214 Change the Service State for a Port" task on page 5-5.
AINS Soak	Automatic in-service soak	Time of presence of valid input signal in hh.mm after which the card is set in service by the software. 0 to 48 hours, 15 minutes increments.

Table 11-6 Line Threshold Options for DS3-12 or DS3N-12 Cards

Parameter	Description	Options
Port #	Port number	1 - 12
CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold 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 bullet and click Show Threshold button.

Table 11-7 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 bullet and click Show Threshold button (Near and Far End, STS termination only).
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).
FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).
UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).

Note The threshold value displays after the circuit is created.

DLP-167 Change Line and Threshold Settings for the DS3E Card

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 not available. If this occurs, remove the DS3E from the ONS 15454, delete the DS-3 card in CTC, and provision the slot for the DS3E (right-click the slot, choose DS3E from the popup menu).

.

Purpose	Use this task to change the line and threshold settings for the DS3E card. The default DS3E values are listed in Table C-3 on page C-8.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Check the type of card installed in ONS 15454 slot. If the DS3E is installed in an ONS 15454 slot that is provisioned for a DS-3 card, the card will appear in CTC as a DS-3 and the DS3E enhanced performance monitoring parameters will not be available. To provision the slot for a DS3E card, see the "NTP-93 Upgrade DS3 Cards to DS3E" procedure on page 12-6.

Step 2 Double-click the DS3E-12 or DS3EN-12 card where you want to change the line or threshold settings.

Step 3 Click the **Provisioning** tab.

Step 4 Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, **Elect Path Thrshld**, or **Sonet Thrshld** subtab.

Note See Chapter 7, "Manage Alarms" for information about the Alarm Behavior tab.

Step 5 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 11-8. For definitions of the Line Threshold settings, see Table 11-9. For definitions of the Electrical Path Thresholds, see Table 11-10. For definitions of the SONET Threshold settings, see Table 11-11.

For the factory default settings for the DS3-12E and DS3N-12E Cards, see Table C-3 on page C-8.

Step 6 Click **Apply**.

Step 7 Repeat Steps 5 and 6 for each subtab that has parameters you want to provision.

Step 8 Return to your originating procedure (NTP).

Table 11-8 Line Options for the DS3-12E and DS3N-12E Cards

Parameter	Description	Options
Port #	Port number	1 - 12 (Read-only)
Port	Port name	User-defined, up to 32 alphanumeric/ special characters. Blank by default. To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
Line Type	Defines the line framing type	• M23 • C Bit • Auto Provisioned
Detected Line Type	Displays the detected line type	Read-only
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 or out of service	See the "DLP-214 Change the Service State for a Port" task on page 5-5.
AINS Soak	Automatic in-service soak	• Time of presence of valid input signal in hh.mm after which the card is set in service by the software. • 0 to 48 hours, 15 minute increments.

Table 11-9 Line Threshold Options for the DS3-12E and DS3N-12E Cards

Subtab	Parameter	Description	Options
Port #	Port number	1 - 12 (Read-only)	Port #
Line Thrshold	CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold 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 bullet and click Show Threshold button.

Table 11-10 Electrical Path Options for the DS3-12E and DS3N-12E Cards

Subtab	Parameter	Description	Options
Port #	Port number	1 - 12 (Read-only)	Port #
Elect Path Thrshld	CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).
	ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (DS3 Pbit: Near End only; DS3 CPbit: Near and Far End).

Table 11-11 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 bullet and click Show Threshold button (Near and Far End, STS termination only).

Table 11-11 SONET Threshold Options for 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 bullet and click Show Threshold button (Near and Far End, STS termination only).
FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).
UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End, STS termination only).

Note The threshold value displays after the circuit is created.

DLP-168 Change Line and Threshold Settings for the DS3XM-6 Card

Note The DS3XM-6 transmux card can accept up to six channelized DS-3 signals and convert each signal to 28 VT1.5s. Conversely, the card can take 28 T-1s and multiplex them into a channeled C-bit or M23 framed DS-3. Unlike the DS3-12, DS3N-12, DS3-12E, and DS3N-12E cards, the DS3XM-6 allows circuit mapping at the VT level.

Purpose	Use this task to change the line and threshold settings for the DS3XM-6 card. The default DS3XM-6 settings are listed in Table C-4 on page C-10.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 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 Thrshld**, **Elect Path Thrshld**, or **Sonet Thrshld** subtab.

Note See Chapter 7, "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 11-12. For definitions of the Line Threshold settings, see Table 11-13. For definitions of the Electrical Path Thresholds, see Table 11-14. For definitions of the SONET Threshold settings, see Table 11-15.

For the factory default settings for the DS3XM-6 Card, see Table C-4 on page C-10.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

Step 7 Return to your originating procedure (NTP).

Table 11-12 Line Options for the DS3XM-6 Parameters

Parameter	Description	Options
Port #	Port number	1 - 6 (read-only)
Port	Port name	User-defined, up to 32 alphanumeric/ special characters. Blank by default To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
Line Type	Defines the line framing type	• M23 - 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 or out of service	See the "DLP-214 Change the Service State for a Port" task on page 5-5
AINS Soak	Automatic in-service soak	• Time of presence of valid input signal in hh.mm after which the card is set in service by the software. • 0 to 48 hours, 15 minutes increments.

Table 11-13 Line Threshold Options for the DS3XM-6 Card

Parameter	Description	Options
Port #	Port number	1 - 6 (read-only)
CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-13 Line Threshold Options for the DS3XM-6 Card (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
LOSS	Loss of signal	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-14 Electrical Path Threshold Options for the DS3XM-6 Card

Parameter	Description	Options
Port #	Port number	1 - 6 (read-only)
CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).

Table 11-14 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 bullet and click Show Threshold button (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 bullet and click Show Threshold button (DS3, Pbit Near End only; DS3 CPbit, Near and Far End; DS1, only if there is a VT circuit dropped on the port).

Table 11-15 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 bullet and click Show Threshold button (STS and VT Term).
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (STS and VT Term).
FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (STS and VT Term).
SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (STS and VT Term).
UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (STS and VT Term).

Note The threshold value displays after the circuit is created.

DLP-169 Change Line and Threshold Settings for the EC-1 Card

Purpose	Use this task to change the line and threshold settings for the EC-1 card. The default EC-1 settings are listed in Table C-5 on page C-13.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 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**, **Thresholds,** or **STS** subtab.

Note See Chapter 7, "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 11-16. For definitions of the threshold settings, see Table 11-17.

For the factory default settings for the EC-1 Card, see Table C-5 on page C-13.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 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 6, "Create Circuits and VT Tunnels." To provision IPPM, go to "DLP-121 Enable Pointer Justification Count Performance Monitoring" task on page 8-2.

Step 7 Return to your originating procedure (NTP).

Table 11-16 Line options for the EC1-12 card

Parameter	Description	Options
Port #	EC-1 card port #	1 - 12 (read-only)
Port Name	Name assigned to the port (optional)	User-defined, up to 32 alphanumeric/ special characters. Blank by default.To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
PJStsMon#	Sets the STS that will be used for pointer justification. If set to zero, no STS is used.	• 0 (default) • 1
Line Length (feet)	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 the port in or out of service	See the "DLP-214 Change the Service State for a Port" task on page 5-5.

Table 11-17 Threshold Options for the EC1-12 Card

SONET Layer	Parameter	Description	Options
	Port #	EC-1 card port #	1 - 12 (read-only)
Line	CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	PPJC-Pdet	Positive Pointer Justification Count, STS Path Detected	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-17 Threshold Options for the EC1-12 Card (continued)

SONET Layer	Parameter	Description	Options
	NPJC-Pdet	Negative Pointer Justification Count, STS Path Detected	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	PPJC-Pgen	Positive Pointer Justification Count, STS Path Generated	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	PSC-W	Protection Switching Count - Working	Threshold values do not apply to the EC1-12 card.
	PSD-W	Protection Switching Duration - Working	Threshold values do not apply to the EC1-12 card.
	PSC-S	Protection Switching Count - Span	Threshold values do not apply to the EC1-12 card.
	PSD-S	Protection Switching Duration - Span	Threshold values do not apply to the EC1-12 card.
	PSC-R	Protection Switching Count - Ring	Threshold values do not apply to the EC1-12 card.
	PSD-R	Protection Switching Duration - Ring	Threshold values do not apply to the EC1-12 card.
Section	CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near End only).
	ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	SEFS	Severely errored framing seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

Table 11-17 Threshold Options for the EC1-12 Card (continued)

SONET Layer	Parameter	Description	Options
Path	CV	Coding violations	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button (Near and Far End).
	ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	FC	Failure count	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	SES	Severely errored seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.
	UAS	Unavailable seconds	Numeric. Can be set for 15 minute or one day intervals. Select bullet and click Show Threshold button.

NTP-89 Modify Line Settings and PM ParameterThresholds for Optical Cards

Purpose	Use this procedure to change the line and threshold settings for optical cards. The default OC-N card settings are provided in the "Card Default Settings" section on page C-4.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-170 Change Line Transmission Settings for OC-N Cards, page 11-20
- DLP-171 Change Threshold Settings for OC-N Cards, page 11-22
- DLP-172 Change an Optical Port to SDH, page 11-25

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-170 Change Line Transmission Settings for OC-N Cards

Purpose	Use this task to change the line transmission settings for OC-N cards. The card default settings are listed in Table C-6 (OC-3), Table C-7 (OC-12), Table C-8 (OC-48) and Table C-9 (OC-192).
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 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 found under this subtab. For definitions of the Line settings, see Table 11-18.

For the factory default settings for the OC-N Cards, see Appendix C, "Network Element Defaults" (see Table C-6 for OC-3 Card default settings, Table C-7 for OC-12 Card default settings, Table C-8 for OC-48 Card default settings, or Table C-9 for OC-192 Card default settings).

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.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

Table 11-18 OC-N Card Line Settings

Parameter	Description	Options
Port #	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.
SF BER Level	Sets the signal fail bit error rate	• 1E-3 • 1E-4 • 1E-5
SD BER Level	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 on the Provisioning > Timing tabs	• Read-only • Yes • No
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
PJ Sts Mon #	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 or out of service	• Out of Service • In Service
Type	Defines the port as SONET or SDH. *Enable Sync Msg* and *Send Do Not Use* must be disabled before the port can be set to SDH.	• Sonet • SDH
AINS Soak	Automatic in-service soak	• Time of presence of valid input signal in hh.mm after which the card is set in service by the software. • 0 to 48 hours, 15 minutes increments.
BLSR Ext	Determines the SONET frame byte used to carry extemded BLSR information	

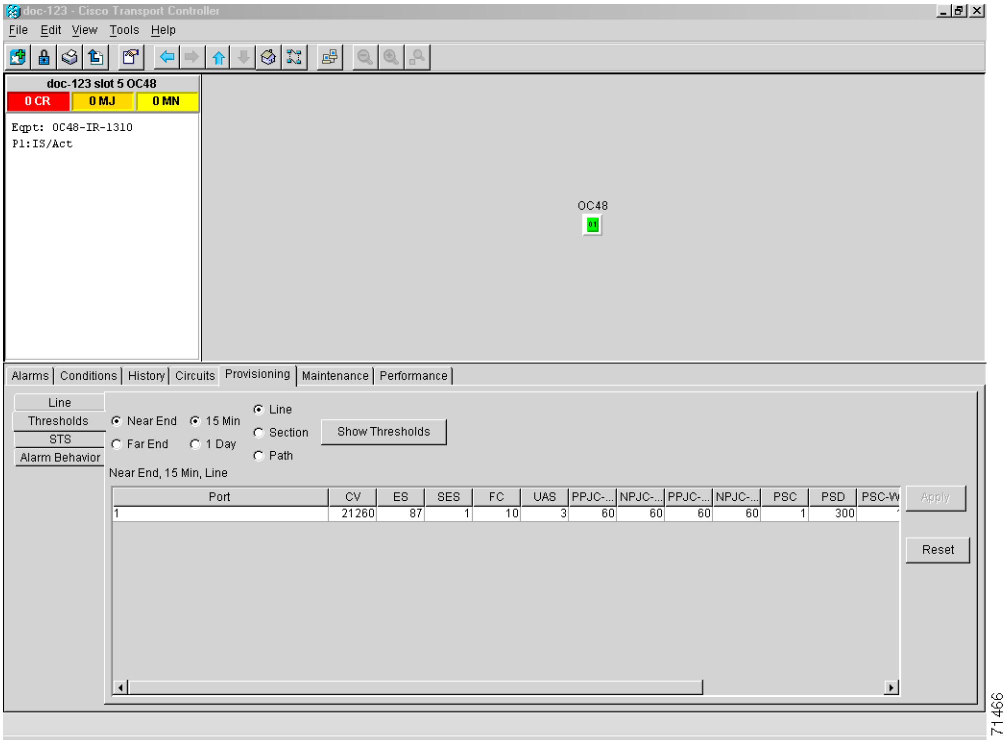
DLP-171 Change Threshold Settings for OC-N Cards

Purpose	Use this task to change threshold settings for OC-N cards. The card default settings are listed in Table C-6 (OC-3), Table C-7 (OC-12), Table C-8 (OC-48) and Table C-9 (OC-192).
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 In node view, double-click the OC-N card where you want to change the threshold settings (Figure 11-2 on page 11-22).

Step 2 Click the **Provisioning > Thresholds** tabs.

Figure 11-2 Provisioning thresholds for the OC48 IR 1310 card



Eqpt: OC48-IR-1310
P1:IS/Act

● Near End ○ Far End
● 15 Min ○ 1 Day
● Line ○ Section ○ Path

Near End, 15 Min, Line

Port	CV	ES	SES	FC	UAS	PPJC-...	NPJC-...	PPJC-...	NPJC-...	PSC	PSD	PSC-W
1	21260	87	1	10	3	60	60	60	60	1	300	

Step 3 Modify any of the settings found under this subtab. For definitions of the Threshold settings, see Table 11-19.

Step 4 For the factory default settings for the OC-N Cards, see Appendix C, "Network Element Defaults" (see Table C-6 for OC-3 Card default settings, Table C-7 for OC-12 Card default settings, Table C-8 for OC-48 Card default settings, or Table C-9 for OC-192 Card default settings).

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

Table 11-19 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 bullet and click Show Threshold button.
ES	Errored seconds	Numeric. Can be set for 15 minute or one day intervals for Line, Section, or Path (Near and Far End). Select bullet and click Show Threshold button.
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 bullet and click Show Threshold button.
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 bullet and click Show Threshold button.
FC	Failure count	Numeric. Can be set for 15 minute or one day intervals for Line . Select bullet and click Show Threshold button. 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 bullet and click Show Threshold button.
PPJC-Pdet	Positive Pointer Justification Count, STS Path detected.	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.
NPJC-Pdet	Negative Pointer Justification Count, STS Path detected.	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.
PPJC-Pgen	Positive Pointer Justification Count, STS Path generated.	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.
NPJC-Pgen	Negative Pointer Justification Count, STS Path generated.	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.

Table 11-19 OC-N Threshold Options (continued)

Parameter	Description	Options
PSC	Protection Switching Count (Line)	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.
PSD	Protection Switch Duration (Line)	Numeric. Can be set for 15 minute or one day intervals for Line (Near and Far End). Select bullet and click Show Threshold button.
PSC-W	Protection Switching Count - Working line 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 bullet and click Show Threshold button.
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 bullet and click Show Threshold button.
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 bullet and click Show Threshold button.
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 bullet and click Show Threshold button.
PSC-R	Protection Switching Duration - 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 bullet and click Show Threshold button.
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 bullet and click Show Threshold button.

DLP-172 Change an Optical Port to SDH

Purpose	Use this task to specify SDH for a port on an OC-N card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Double-click the OC-N card where you want to set a port to SDH.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Under Type, specify the port and choose SDH.

Note Before you can set *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, and the card is not a SONET DCC termination point.

Step 4 Click **Apply**.

Step 5 If the card is a multiport OC-N card, such as an OC12-4, you can repeat Steps 3 and 4 for any other ports on that card that you want to set to SDH.

Step 6 Return to your originating procedure (NTP).

NTP-90 Modify Alarm Interface Controller Settings

Purpose	Use this procedure to provision the AIC card to receive input from, or send output to, external devices wired to the backplane (called external alarms and controls).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Note If the AIC card is being provisioned for the first time, see the "NTP-32 Provision the Alarm Interface Controller" procedure on page 4-31.

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-173 Change External Alarms Using the AIC, page 11-26

- DLP-174 Change External Controls Using the AIC, page 11-27
- DLP-175 Change Orderwire Settings Using the AIC, page 11-28

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-173 Change External Alarms Using the AIC

Purpose	Use this task to change external alarm settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-19 Install Alarm Wires on the Backplane" task on page 1-36 for more information.

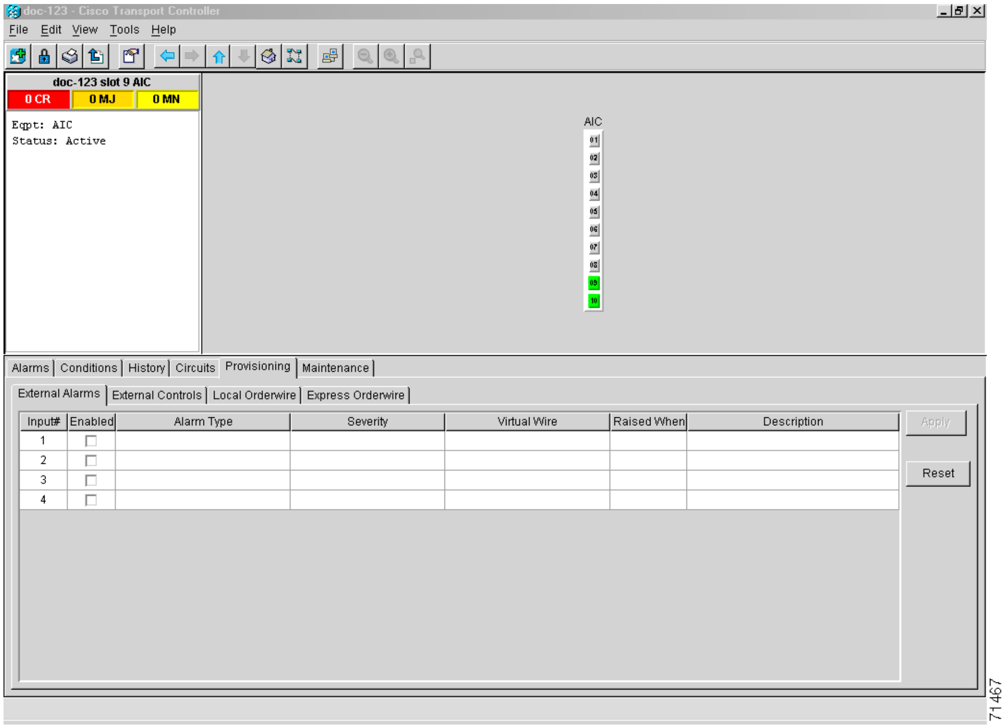
Step 2 Double-click the AIC to display it in card view.

Step 3 Click the **Provisioning > External Alarms** tabs (Figure 11-3 on page 11-27).

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 "DLP-82 Provision External Alarms and Controls" task on page 4-32.

- Enabled
- Alarm Type
- Severity
- Virtual Wire
- Raised When
- Description

Figure 11-3 Provisioning external alarms on the AIC card



Eqpt: AIC
Status: Active

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	□					
2	□					
3	□					
4	□					

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-174 Change External Controls Using the AIC

Purpose	Use this task to change external control settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-19 Install Alarm Wires on the Backplane" task on page 1-36 for more information.

Step 2 Double-click the AIC 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 "DLP-82 Provision External Alarms and Controls" task on page 4-32.

- 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-175 Change Orderwire Settings Using the AIC

Purpose	Use this task to change orderwire settings on the AIC card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

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 Double-click the AIC to display it in card view.

Step 2 Select the **Local Orderwire** or **Express Orderwire** subtab, depending on the orderwire path that you want to create.

The Local Orderwire subtab is shown in Figure 11-5 on page 11-32. The example shows the subtab for the AIC-I card. The screen for the AIC card is similar. 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 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-118 Modify Alarm Interface Controller-International Settings

Purpose	Use this procedure to provision the AIC-I card to receive input from, or send output to, external devices wired to the backplane (called external alarms and controls), or to change orderwire settings.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Note If the AIC-I card is being provisioned for the first time, see the "NTP-123 Provision the Alarm Interface Controller-International" procedure on page 4-35.

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-208 Change External Alarms Using the AIC-I, page 11-29
- DLP-209 Change External Controls Using the AIC-I, page 11-31
- DLP-210 Change AIC-I Orderwire Settings, page 11-31

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-208 Change External Alarms Using the AIC-I

Purpose	Use this task to change external alarm settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-19 Install Alarm Wires on the Backplane" task on page 1-36 for more information.

Step 2 Double-click the AIC-I to display it in card view.

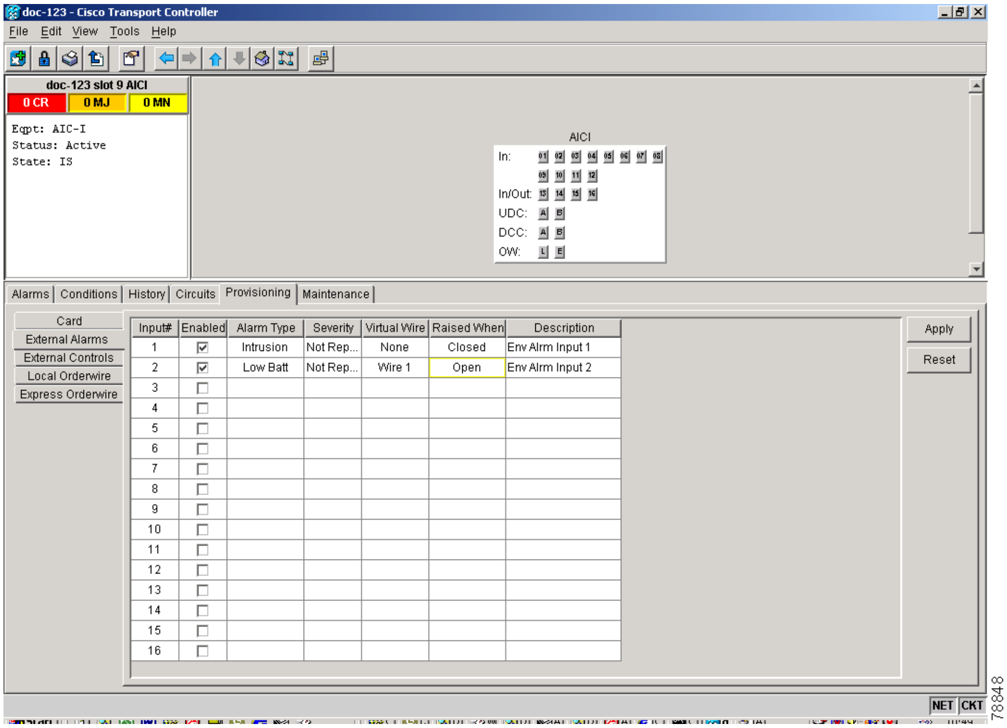
Step 3 Click the **Provisioning > External Alarms** tabs (Figure 11-4 on page 11-30).

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 "DLP-211 Provision External Alarms and Controls on the AIC-I Card" task on page 4-36.

- Enabled

- Alarm Type
- Severity
- Virtual Wire
- Raised When
- Description

Figure 11-4 Provisioning external alarms on the AIC-I card



Eqpt: AIC-I
Status: Active
State: IS

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	☑	Intrusion	Not Rep...	None	Closed	Env Alrm Input 1
2	☑	Low Batt	Not Rep...	Wire 1	Open	Env Alrm Input 2
3	☐					
4	☐					
5	☐					
6	☐					
7	☐					
8	☐					
9	☐					
10	☐					
11	☐					
12	☐					
13	☐					
14	☐					
15	☐					
16	☐					

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).

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.

DLP-209 Change External Controls Using the AIC-I

Purpose	Use this task to change external control settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-19 Install Alarm Wires on the Backplane" task on page 1-36 for more information.

Step 2 Double-click the AIC-I 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 "DLP-82 Provision External Alarms and Controls" task on page 4-32.

- 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).

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.

DLP-210 Change AIC-I Orderwire Settings

Purpose	Use this task to change orderwire settings on the AIC-I card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

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.

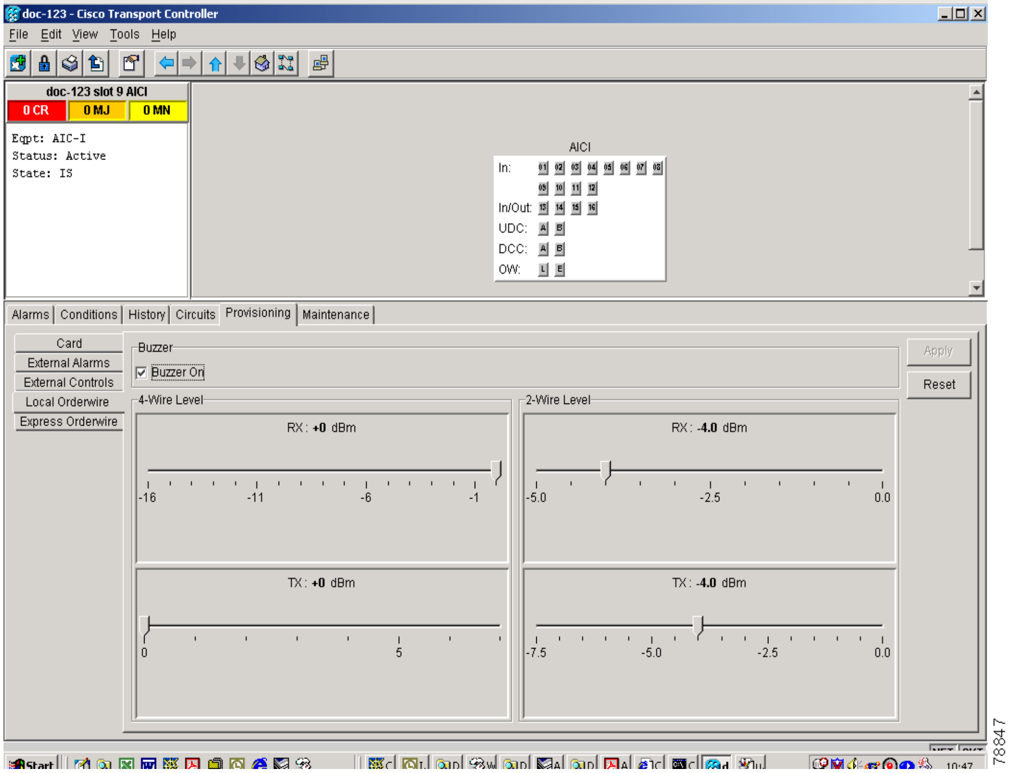
Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1 Double-click the AIC-I to display it in card view.

Step 2 Select the **Local Orderwire** or **Express Orderwire** subtab, depending on the orderwire path that you want to create.

The Local Orderwire subtab is shown in Figure 11-5 on page 11-32. Provisioning steps are the same for both types of orderwire.

Figure 11-5 Provisioning local orderwire



doc-123 - Cisco Transport Controller

doc-123 slot 9 AICI

0 CR 0 MJ 0 MN

Eqpt: AIC-I
Status: Active
State: IS

☑ Buzzer On

4-Wire Level: RX: +0 dBm; TX: +0 dBm

2-Wire Level: RX: -4.0 dBm; TX: -4.0 dBm

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-91 Upgrade DS-1 and DS-3 Protect Cards from 1:1 Protection to 1:N Protection

Purpose	Use this task to convert DS-1 and DS-3 protect cards from 1:1 to 1:N protection.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Log into the ONS 15454 node where you want to change the settings. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

Step 3 Perform any of the following tasks as needed:

- DLP-176 Convert DS1-14 Cards From 1:1 to 1:N Protection, page 11-33
- DLP-177 Convert DS3-12 Cards From 1:1 to 1:N Protection, page 11-35

Step 4 Complete the "NTP-108 Back Up the Database" procedure on page 15-7.

DLP-176 Convert DS1-14 Cards From 1:1 to 1:N Protection

Purpose	Use this task to convert DS1-14 cards in a 1:1 protection scheme to 1:N protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite

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 and a protection group with DS1-14 cards.

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 in Figure 11-5 on page 11-34) and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to 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 – 3 for each protection group that you need to convert.

Step 5 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 displays, 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 – 9 for other protection groups.

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 pull-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 pull-down menu, choose **1:N (card)**.

Step 20 From the Protect Card pull-down menu, choose the DS1N-14 card. Verify that the correct DS1N-14 card appears in the Protect Card field.

Step 21 Under Available Cards, 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 pull-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-177 Convert DS3-12 Cards From 1:1 to 1:N Protection

Purpose	Use this task to convert DS3-12 cards in a 1:1 protection scheme to 1:N protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite

Note This procedure assumes that DS3-12 cards are installed in Slots 1 - 6 and/or Slots 12 - 17. The DS3-12 cards in Slots 3 and 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 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 in Figure 11-5 on page 11-34, and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to 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 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 displays, 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 protection group, repeat Steps 7 – 9 for each group.

Step 11 Physically remove the 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 pull-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.

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 pull-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-178 Convert DS3-12E Cards From 1:1 to 1:N Protection

Purpose	Use this task to convert DS3-12E cards in a 1:1 protection scheme to 1:N protection.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite

Note This procedure assumes that DS3-12E cards are installed in Slots 1 - 6 and/or Slots 12 - 17. The DS3-12E cards in Slots 3 and 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** tabs.

Step 2 Click the protection group containing 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 in Figure 11-5 on page 11-34, and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to 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 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** 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 displays, 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 protection group, repeat Steps 7 – 9 for each group.

Step 11 Physically remove the 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 pull-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 pull-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).

Upgrade Cards and Spans

This chapter explains how to upgrade cross-connect (XC, XCVT, XC10G) cards, DS3 and DS3N cards, and optical spans within a ring or protection group.

Before You Begin

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

1. NTP-92 Upgrade Cross-Connect Cards, page 12-1—Complete this procedure as needed to upgrade XC, XCVT, or XC10G cards.
2. NTP-93 Upgrade DS3 Cards to DS3E, page 12-6— Complete this procedure as needed to upgrade DS3 or DS3N cards to DS3E or DS3N-E cards.
3. NTP-153 Upgrade the AIC Card to AIC-I, page 12-9—Complete this procedure as need to upgrade the Alarm Interface Controller (AIC) card to the AIC-International (AIC-I).
4. NTP-94 Upgrade Optical Spans Automatically, page 12-9—Complete this procedure as needed to upgrade optical cards within UPSRs, BLSRs, and 1+1 protection groups.
5. NTP-95 Upgrade Optical Spans Manually, page 12-13—Complete this procedure as needed to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).

NTP-92 Upgrade Cross-Connect Cards

Purpose	This procedure describes how to upgrade XC and XCVT cards.
Tools/Equipment	Replacement cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Step 1 Log into the node where you will perform the XC/XCVT upgrade. The node (default) view displays. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Complete the "DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades" task on page 12-2.

Step 3 Based on the card you are upgrading, complete the applicable task:

- DLP-180 Upgrade the XC Card to the XCVT Card, page 12-3
- DLP-181 Upgrade the XC/XCVT Card to the XC10G Card, page 12-4

DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades

Purpose	This task prevents a linear 1+1, UPSR, or BLSR protection switch from occurring during XC/XCVT upgrades.
Tools/Equipment	Replacement cross-connect card
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Step 1 Ensure the working span is working/active on both local and remote nodes according to the specific protection scheme:

a. For a BLSR protection scheme:

– In node view, click the **Maintenance > BLSR** tabs.

– Locate the applicable span.

– In the West Line and East Line columns, the working/active span is identified by Work/Act.

b. For a 1+1 protection scheme:

– In node (default) view, click the **Maintenance > Protection** tabs.

– Locate the applicable 1+1 protection group and make sure the status is Working/Active and Protect/Standby, rather than Working/S

c. For a UPSR protection scheme, no verification is necessary.

Step 2 Ensure the working span is carrying error-free traffic (no SD or SF alarms present):

a. Display the network view and click the **Alarms** tab to display alarms.

b. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Lockout the protection span according to the specific protection scheme:

a. Lockout the protection span in a BLSR protection scheme:

– In node (default) view, click the **Maintenance > BLSR** tabs.

– Locate the applicable span.

– In the West Line and East Line columns, the working/active span is identified by (Work/Act). Place a lockout on the East and West cards of the nodes adjacent to the XC switch node by clicking on the fields under those columns and choosing **LOCKOUT SPAN**; for example, to switch the XC on Node B, place a lockout on the West card of Node A and on the East card of Node C, no lockout is necessary on Node B. Before the lockout is set, verify that the BLSR is not switched. If a lockout is set while the BLSR is switched, traffic can be lost.

<------East [Node A] West------East [Node B] West------East [Node C] West------>

b. Lockout the protection span in a 1+1 protection scheme:
   - In node (default) view, click the **Maintenance > Protection** tabs.
   - Choose the affected 1+1 protection group from the Protection Groups window.
   - In the Selected Group window, the working and protect spans appear. Choose the **protect/standby card** and choose **Lockout** from the inhibit switching row.
   - Click **Yes** on the confirmation dialog box.

c. Switch traffic to one span in a UPSR protection scheme:
   - Complete the "DLP-197 Switch UPSR Traffic" task on page 14-18 to apply a force switch on the span that will be upgraded.

Step 4 The protection span is now locked out. Complete the "DLP-180 Upgrade the XC Card to the XCVT Card" task on page 12-3 or the "DLP-181 Upgrade the XC/XCVT Card to the XC10G Card" task on page 12-4 and release the protection lock out when indicated in either task.

DLP-180 Upgrade the XC Card to the XCVT Card

Purpose	This task upgrades the XC card to the XCVT card
Tools/Equipment	Two XCVT cards
Prerequisite Procedures	DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades, page 12-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note The UNEQ-P alarm can be raised during a cross-connect card upgrade if you have E100/E1000 cards in the system. The alarm will appear and clear within a few seconds.

Step 1 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.

Note You can also place the cursor on the card graphic in CTC to display a dialog. This display identifies the card as XC: Active or XC: Standby.

Step 2 Physically replace the standby XC card on the ONS 15454 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 ACT/STBY LED turns amber and remains illuminated.

Step 3 In node view, click the **Maintenance > XC Cards** tabs.

Step 4 From the Cross Connect Cards menu, choose **Switch**.

Step 5 Click **Yes** on the Confirm Switch dialog box. Traffic switches to the XCVT card you inserted in Step 2. The ACT/STBY LED on this card changes from amber to green.

Note The Interconnection Equipment Failure alarm will be displayed, but will clear when the upgrade procedure is complete and the node has matching cross-connect cards installed.

Step 6 Physically remove the now standby XC card from the ONS 15454 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.

Step 7 Complete the "DLP-203 Clear a Lock On or Lock Out" task on page 15-19 to release the protection lockout(s) you applied in the "DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades" task on page 12-2.

DLP-181 Upgrade the XC/XCVT Card to the XC10G Card

Purpose	This task upgrades the XC/XCVT card to the XC10G card.
Tools/Equipment	Two XC10G cards
Prerequisite Procedures	DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades, page 12-2 DLP-60 Log into CTC, page 3-22
Required/As Needed	Software release 3.1 and later and the 15454-SA-ANSI shelf are required for XC10G operation.
Onsite/Remote	Onsite
Security Level	Maintenance or higher

Note This procedure only applies to XC/XCVT cards that are installed in the 15454-SA-ANSI (Software R3.1 and later). You cannot perform this upgrade from shelves released prior to software R3.1. The XC10G requires the 15454-SA-ANSI.

Note The UNEQ-P alarm can be raised during a cross-connect card upgrade if you have E100T-12/E1000-2 cards in the node. The alarm will appear and clear within a few seconds.

Step 1 Determine the standby XC/XCVT card. The ACT/STBY LED of the standby XC/XCVT card is amber, while the ACT/STBY LED of the active XC/XCVT card is green.

Note You can also place the cursor on the card graphic in CTC to display a dialog. This display identifies the card as XC/XCVT: Active or XC/XCVT: Standby.

Step 2 Physically replace the standby XC/XCVT card on the ONS 15454 with an XC10G card:

a. Open the XC/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.

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 illuminated.

Step 3 In node view, click the **Maintenance > XC Cards** tabs.

Step 4 From the Cross Connect Cards menu, choose **Switch**.

Step 5 Click **Yes** on the Confirm Switch dialog box. Traffic switches to the XC10G card you inserted in Step 2. The ACT/STBY LED on this card changes from amber to green.

Note The Interconnection Equipment Failure alarm will be displayed, but will clear when the upgrade procedure is complete and the node has matching cross-connect cards installed.

Step 6 Physically remove the now standby XC/XCVT card from the ONS 15454 and insert the second XC10G card into the empty XC/XCVT slot:

a. Open the XC/XCVT card ejectors.

b. Slide the XC/XCVT card out of the slot.

c. Open the ejectors on the XC10G.

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.

Step 7 Complete the "DLP-203 Clear a Lock On or Lock Out" task on page 15-19 to release the protection lockout(s) you applied in the "DLP-234 Prevent a Protection Switch During Cross-Connect Card Upgrades" task on page 12-2.

NTP-93 Upgrade DS3 Cards to DS3E

Purpose	Use these tasks to upgrade DS3 cards to DS3E cards or to downgrade from DS3E cards to DS3 cards.
Tools/Equipment	Replacement cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Upgrading to DS3E or DS3EN cards requires that the ONS 15454 is running CTC Release 3.1 or later. 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 DS3E card upgrade supports 1:1 and 1:N protection schemes. The procedure is non-service affecting, that is, the upgrade will cause a switch less than 50 ms in duration.

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22. The node (default) view displays.

Step 2 If you need to upgrade a DS3 (DS3N) card to a DS3E (DS3EN) card, complete the "DLP-182 Upgrade the DS3/DS3N Card to the DS3E/DS3EN Card" task on page 12-6.

Note This procedure can also be used to enable the capabilities of a DS3E card that was installed in a shelf with Software R3.1 or earlier.

Step 3 If you need to downgrade a DS3 or DS3E card, complete the "DLP-183 Downgrade a DS3E/DS3NE Card to a DS3/DS3N Card" task on page 12-8. The procedure for downgrading is the same as upgrading except you choose DS3 or DS3N from the Change Card pull-down menu.

DLP-182 Upgrade the DS3/DS3N Card to the DS3E/DS3EN Card

Purpose	This task upgrades the DS3 card to the DS3E card or the DS3N card to the DS3EN card.
Tools/Equipment	DS3E or DS3EN card
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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 will be raised and will clear on their own; however, there should be no Service-Affecting (SA, Major, or Critical) alarms. If any Service-Affecting alarms occur, Cisco recommends backing out of the procedure.

Step 1 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 (i.e., 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.

Step 2 If the card you are upgrading is unprotected, skip to Step 3. If the card you are upgrading is protected, complete the "DLP-202 Apply a Lock Out" task on page 15-18 on the protect card.

Note Traffic will be lost during an upgrade on an unprotected card.

Step 3 Physically remove the protect DS3 or the protect DS3N card:

a. Open the DS3/DS3N card ejectors.

b. Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the upgrade is complete.

Step 4 Right-click the protect slot and choose **Change Card** from the pull-down menu.

Step 5 Choose the new card (DS3E or DS3EN) from the Change to: pull-down menu.

Step 6 Click **OK**.

Step 7 Insert the new DS3E or DS3EN card into the protect slot:

a. Open the ejectors on the DS3E/DS3EN card.

b. Slide the DS3E/DS3EN card into the slot along the guide rails.

Step 8 Close the ejectors.

Wait for the IMPROPRMVL alarm to clear and the card to become standby.

Step 9 If you placed a lock out on the protect card in Step 2, complete the "DLP-203 Clear a Lock On or Lock Out" task on page 15-19 to remove the lockout.

Step 10 Repeat this task (Steps 1–9) for the working card.

Note After upgrading from a DS3 to DS3E card, check the DS3E line type is set to the framing type employed by your particular SONET network to take full advantage of the performance monitoring capabilities of the DS3E. At the CTC card level, click the **Provisioning > Line** tabs and check the Line Type column.

Step 11 Return to your originating procedure (NTP).

DLP-183 Downgrade a DS3E/DS3NE Card to a DS3/DS3N Card

Purpose	This task downgrades a DS3E or DS3NE card. Downgrading can be performed to back out of an upgrade.
Tools	None
Prerequisite Procedures	DLP-182 Upgrade the DS3/DS3N Card to the DS3E/DS3EN Card, page 12-6 DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note All ports must be provisioned as UNFRAMED and not have the Path Trace enabled.

Note Working cards must be downgraded before protect cards.

Tip The procedure for downgrading is the same as upgrading except you choose DS3 or DS3N from the Change Card pull-down menu.

Step 1 Determine if the card you are downgrading is protected or unprotected:

- **a.** A protected card will be listed under Protection Groups in the **Maintenance > Protection** tabs. The slot, port and status (i.e., 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.

Step 2 If the card you are downgrading is unprotected, skip to Step 3. If the card you are downgrading is protected, complete the "DLP-202 Apply a Lock Out" task on page 15-18 for working card.

Step 3 Physically remove the working DS3E or the working DS3EN card:

- **a.** Open the DS3E/DS3EN card ejectors.
- **b.** Slide the card out of the slot. This raises the IMPROPRMVL alarm, which will clear when the downgrade is complete.

Step 4 Right-click the slot to be downgraded and choose **Change Card** from the pull-down menu.

Step 5 Choose **DS3** or **DS3N** from the Change to: pull-down menu.

Step 6 Click **OK**.

Step 7 Insert the DS3 or DS3N card into the working slot:

- **a.** Open the ejectors on the DS3/DS3N card.
- **b.** Slide the DS3/DS3N card into the slot along the guide rails.

Step 8 Close the ejectors. Wait for the IMPROPRMVL alarm to clear and the card to become active.

Step 9 If you placed a lockout on the working card in Step 2, complete the "DLP-203 Clear a Lock On or Lock Out" task on page 15-19 to remove the lockout.

Step 10 Repeat Steps 1–9 to downgrade the protect card if applicable.

Step 11 Return to your originating procedure (NTP).

NTP-153 Upgrade the AIC Card to AIC-I

Purpose	This task upgrades an AIC to an AIC-I to provide more alarm contacts.
Tools	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite

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-38 Install the Alarm Interface Controller or Alarm Interface Controller-International Card" task on page 2-10.

NTP-94 Upgrade Optical Spans Automatically

Purpose	Use this procedure to upgrade OC-N speeds within BLSRs, UPSRs, and 1+1 protection groups using the Span Upgrade Wizard.
Tools/Equipment	Replacement cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22. The node (default) view displays.

Step 2 Complete the "DLP-184 Perform a Span Upgrade Using the Span Upgrade Wizard" task on page 12-10 to upgrade an optical span within a BLSR, UPSR, or 1+1 protection group. Valid span upgrades include:

- 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

Note You cannot upgrade a four-port OC-12 span.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15454 Reference Manual*.

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 Span upgrades do not upgrade SONET topologies; for example, a 1+1 protection group to a two-fiber BLSR.

Note During the upgrade/downgrade some minor alarms and conditions will be raised and will clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSR Out of Sync, 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 Out of Sync alarms. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

DLP-184 Perform a Span Upgrade Using the Span Upgrade Wizard

Purpose	This task upgrades two-fiber BLSR spans, four-fiber BLSR spans, UPSR 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
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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.

Caution If you want to upgrade all of the spans in a ring, determine if there are any four-port OC-12 cards in the ring. If the ring contains any OC-12-4 cards and you wish to continue with the upgrade, you will have 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).

Note An OC-12 to four-port OC-12 span upgrade can only be performed from multispeed slots (slots 1–4 and 14–17) because the four-port OC-12 card can only be installed in multispeed slots. Ensure the OC-12 cards are in multispeed slots before performing a span upgrade to the four-port OC-12. The OC-12 port will be mapped to port 1 on the four-port OC-12.

Note The Span Upgrade option will only be visible and available if the hardware and hardware compatibility 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 the span. In the case of an OC-12 to OC12-4 span upgrade, the OC12-4 option will not be visible or available if the OC12 cards are in high speed slots, even if XC10G cards are installed, because OC12-4 cards are only supported in multispeed slots.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present:

a. Navigate from the default (node) view to the network view by clicking on the Go To Network View button in the tool bar.

b. In network view, click on the **Alarms** tab to view a list of current alarms.

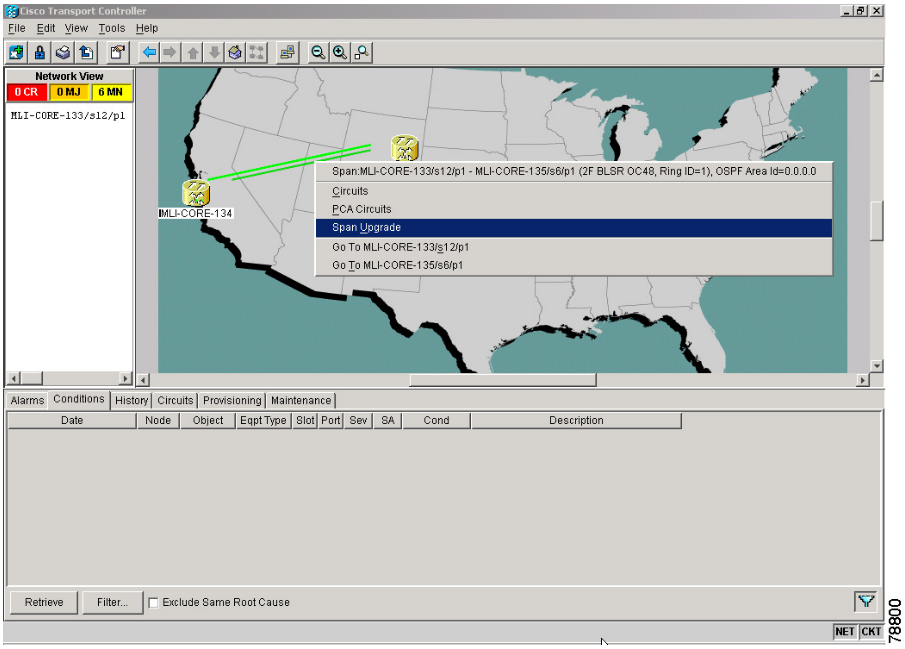
c. In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition (including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING) is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 In network view, right-click the span you want to upgrade.

Step 3 Choose **Span Upgrade** from the pull-down menu (Figure 12-1).

Figure 12-1 Span Upgrade pull-down menu

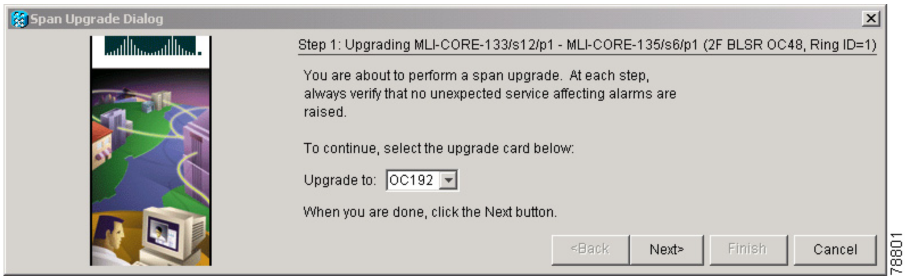


Span:MLI-CORE-133/s12/p1 - MLI-CORE-135/s6/p1 (2F BLSR OC48, Ring ID=1), OSPF Area Id=0.0.0.0

Step 4 The first Span Upgrade dialog box appears (Figure 12-2). 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 12-2 Beginning the Span Upgrade Wizard



Step 1: Upgrading MLI-CORE-133/s12/p1 - MLI-CORE-135/s6/p1 (2F BLSR OC48, Ring ID=1)

You are about to perform a span upgrade. At each step, always verify that no unexpected service affecting alarms are raised.

To continue, select the upgrade card below:

Upgrade to: OC192

When you are done, click the Next button.

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 If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Note Remember to attach the fiber after installing the OC-N cards.

Step 5 Repeat Steps 2–4 for additional spans in the ring.

Step 6 Return to your originating procedure (NTP).

NTP-95 Upgrade Optical Spans Manually

Purpose	Use this procedure to upgrade OC-N speeds within BLSRs, UPSRs, and 1+1 protection groups by upgrading OC-N cards.
Tools/Equipment	Replacement cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution If you want to upgrade all of the spans in a ring, determine if there are any four-port OC-12 cards in the ring. If the ring contains any OC-12-4 cards and you wish to continue with the upgrade, you will have 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).

Note Optical card transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15454 Reference Manual*.

Note In this context the word “span” represents the optical path between two nodes. The words “span endpoint” represent the nodes on each end of a span.

Step 1 Complete the “DLP-60 Log into CTC” task on page 3-22. The node (default) view displays.

Step 2 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):

- Complete the “DLP-235 Perform a Manual Span Upgrade on a Two-Fiber BLSR” task on page 12-15 to manually upgrade an optical span within a two-fiber BLSR.
- Complete the “DLP-236 Perform a Manual Span Upgrade on a Four-Fiber BLSR” task on page 12-17 to manually upgrade an optical span within a four-fiber BLSR.
- Complete the “DLP-187 Perform a Manual Span Upgrade on a UPSR” task on page 12-19 to manually upgrade an optical span within a two-fiber UPSR.
- Complete the “DLP-188 Perform a Manual Span Upgrade on a 1+1 Protection Group” task on page 12-20 to manually upgrade an optical span within a 1+1 protection group.

- Complete the "DLP-237 Perform a Manual Span Upgrade on an Unprotected Span" task on page 12-22 to manually upgrade an unprotected optical span.

Valid span upgrades include:

- 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

Note You cannot upgrade a four-port OC-12 span.

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 Span upgrades do not upgrade SONET topologies; for example, a 1+1 protection group to a two-fiber BLSR.

Note If you are upgrading a span on a BLSR, a BLSROSYNC alarm will appear in the alarms list. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for information on this alarm.

Note During the upgrade/downgrade some minor alarms and conditions will be raised and will clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSR Out of Sync, 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 Out of Sync alarms. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

Note The Span Upgrade option will only be visible and available if the hardware and hardware compatibility 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 f the span. In the case of an OC12 to OC12-4 span upgrade, the OC12-4 option will not be visible or available if the OC12 cards are in high speed slots, even if XC10G cards are installed, because OC12-4 cards are only supported in multispeed slots.

DLP-235 Perform a Manual Span Upgrade on a Two-Fiber BLSR

Purpose	This task upgrades a two-fiber BLSR span to a higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 If any of the cross-connect cards reboot during the span upgrade, you must manually reset each one once the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-113 Reset the TCC+ Using CTC" task on page 15-24 for card reset procedures.

Note All spans connecting the nodes in a BLSR must be upgraded before the added bandwidth is available.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade:

a. Navigate from the default (node) view to the network view.

b. In network view, click the **Alarms** tab to view a list of current alarms.

c. In network view, click the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 Apply a force switch to both span endpoints (nodes) on the span that you will upgrade first:

a. At the first endpoint, in node view, click the **Maintenance > BLSR** tabs.

b. Click the West Switch or the East Switch field and choose **FORCE RING** from the menu.

c. Click **Apply**.

d. At the second endpoint, in node view, click the **Maintenance > BLSR** tabs.

e. Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.

f. Click **Apply**.

Note A force switch request on a span or card causes CTC to raise a FORCED-REQ condition. It is informational only; the condition will clear when the force switch command is cleared.

Step 3 Remove the fiber from both endpoints and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both endpoints.

Step 5 From both endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N type.

Step 7 Click **OK**.

Step 8 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.

Note If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Step 9 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:

a. At the first endpoint, in node view, click the **Maintenance > BLSR** tabs.

b. Click the West Switch or the East Switch field and choose **CLEAR** from the menu.

c. Click **Apply**.

d. At the second endpoint, in node view, click the **Maintenance > BLSR** tabs.

e. Click the West Switch or the East Switch field and choose **CLEAR** from the menu.

f. Click A**pply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10 Repeat this task for each span in the BLSR. When you are done with each span, the upgrade is complete.

Step 11 Return to your originating procedure (NTP).

DLP-236 Perform a Manual Span Upgrade on a Four-Fiber BLSR

Purpose	This task upgrades a four-fiber BLSR span to a higher optical rate. Repeat the task to upgrade each span, and thus the whole ring, to the higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 If any of the cross-connect cards reboot during the span upgrade, you must manually reset each one once the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-113 Reset the TCC+ Using CTC" task on page 15-24 for card reset procedures.

Note All spans connecting the nodes in a BLSR must be upgraded before the added bandwidth is available.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade:

a. Navigate from the default (node) view to the network view.

b. In network view, click on the **Alarms** tab to view a list of current alarms.

c. In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 Apply a force switch to both span endpoints (nodes) on the span that you will upgrade first:

a. At the first endpoint (node), in node view, click the **Maintenance > BLSR** tabs.

b. Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.

c. Click **Apply**.

d. At the second endpoint (node), in node view, click the **Maintenance > BLSR** tabs.

e. Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.

f. Click **Apply**.

Note A force switch request on a span or card causes CTC to raise a FORCED-REQ condition. It is informational only; the condition will clear when the force switch command is cleared.

Step 3 Remove the fiber from both working and protect cards at both span endpoints (nodes) and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both end points.

Step 5 For both ends of the span endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N type.

Step 7 Click **OK**.

Step 8 When you have finished Step 5–7 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.

Note If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Step 9 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:

a. At the first endpoint (node), in node view, click the **Maintenance > BLSR** tabs.

b. Click the West Switch or the East Switch field and choose **CLEAR** from the menu.

c. Click **Apply**.

d. At the second endpoint (node), in node view, click the **Maintenance > BLSR** tabs.

e. Click the West Switch or the East Switch field and choose **CLEAR** from the menu.

f. Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10 Repeat these steps for each span in the BLSR. When all spans in the BLSR have been upgraded, the ring is upgrade.

Step 11 Return to your originating procedure (NTP).

DLP-187 Perform a Manual Span Upgrade on a UPSR

Purpose	This task upgrades UPSR spans to a higher optical speed. Repeat the task to upgrade each span, and thus the entire ring, to the higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 If any of the cross-connect cards reboot during the span upgrade, you must manually reset each one, once the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-113 Reset the TCC+ Using CTC" task on page 15-24 for card reset procedures.

Note An OC-12 to four-port OC-12 span upgrade can only be performed from multispeed slots (slots 1–4 and 14–17) because the four-port OC-12 card can only be installed in multispeed slots. Ensure the OC-12 cards are in multispeed slots before performing a span upgrade to the four-port OC-12. The OC-12 port will be mapped to port 1 on the four-port OC12.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:

a. Navigate from the default (node) view to the network view.

b. In network view, click on the **Alarms** tab to view a list of current alarms.

c. In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 Complete the "DLP-197 Switch UPSR Traffic" task on page 14-18 to apply a force switch on the span that you will upgrade.

Step 3 Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both span endpoints.

Step 5 For both ends of the span, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N type.

Step 7 Click **OK**.

Step 8 When you have finished Step 5–7 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.

Note If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Step 9 Complete the "DLP-198 Clear a UPSR Traffic Switch" task on page 14-19 when cards on each side of the span have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 10 Return to your originating procedure (NTP).

DLP-188 Perform a Manual Span Upgrade on a 1+1 Protection Group

Purpose	This task upgrades a 1+1 protection group span.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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 If any of the cross-connect cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-113 Reset the TCC+ Using CTC" task on page 15-24 for card reset procedures.

Note If the switching mode is bidirectional in the 1+1 protection group, apply the Force command to only one end of the span, not both. If the Force command is applied to both ends when the switching mode is bidirectional, it will cause a switch of more than 50 ms in duration. Clear the force command at the same end it was applied.

Note An OC-12 to four-port OC-12 span upgrade can only be performed from multispeed slots (slots 1–4 and 14–17) because the four-port OC-12 card can only be installed in multispeed slots. Ensure the OC-12 cards are in multispeed slots before performing a span upgrade to the four-port OC-12. The OC-12 port will be mapped to port 1 on the four-port OC12.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:

a. Navigate from the default (node) view to the network view.

b. In network view, click on the **Alarms** tab to view a list of current alarms.

c. In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 Apply a force switch on the ports that you will upgrade, beginning with the protect port:

a. In node view, click the **Maintenance > Protection** tabs.

b. Under Protection Groups, choose the 1+1 protection group.

c. Under Selected Group, choose the protect port (regardless if it is active or standby).

d. From Switch Commands, click **Force**.

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

Note A force switch request on a span or card (port) causes CTC to raise a FORCED-REQ condition. It is informational only; the condition will clear when the force switch command is cleared.

Step 3 Repeat Step 2 for each port you will upgrade.

Step 4 Remove the fiber from both ends of the span and ensure that traffic is still running.

Step 5 Remove the OC-N cards from both span endpoints.

Step 6 At both ends of the span, in node view, right-click the OC-N slot and choose **Change Card**.

Step 7 In the Change Card dialog box, choose the new OC-N type.

Step 8 Click **OK**.

Step 9 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 standby.

Note If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Step 10 When cards on each end of the line have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:

a. In node view, click the **Maintenance > Protection** tabs.

b. Under Protection Groups, choose the 1+1 protection group.

c. Under Selected Group, choose the port with the force on it.

d. From Switch Commands, click **Clear**.

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

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card.

Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Step 11 Repeat this task for the other line in the 1+1. When the other line in the 1+1 has been upgraded, the span upgrade is complete.

Step 12 Return to your originating procedure (NTP).

DLP-237 Perform a Manual Span Upgrade on an Unprotected Span

Purpose	This task manually upgrades unprotected spans to a higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
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.

Note If any of the cross-connect cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-113 Reset the TCC+ Using CTC" task on page 15-24 for card reset procedures.

Note An OC-12 to four-port OC-12 span upgrade can only be performed from multispeed slots (slots 1–4 and 14–17) because the four-port OC-12 card can only be installed in multispeed slots. Ensure the OC-12 cards are in multispeed slots before performing a span upgrade to the four-port OC-12. The OC-12 port will be mapped to port 1 on the four-port OC12.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, and SD, are present on the span that you will upgrade:

a. Navigate from the default (node) view to the network view.

b. In network view, click the **Alarms** tab to view a list of current alarms.

c. In network view, click the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 2 Remove the fiber from both endpoint nodes in the span.

Caution Removing the fiber will cause all traffic on the unprotected span to be lost.

Step 3 Remove the OC-N cards from both span endpoints.

Step 4 For both ends of the span, in node view, right-click on each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N type.

Step 6 Click **OK**.

Step 7 When you have finished Steps 4 – 6 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.

Note If you install OC-192 cards, a disabled OC-192 laser causes an LOS alarm to be reported for each OC-192 slot. Enable the OC-192 laser by setting the safety key lock on the OC-192 faceplate to the ON position (labeled 1).

Step 8 Return to your originating procedure (NTP).

CHAPTER 13

Upgrade Network Configurations

This chapter explains how to upgrade from one SONET topology to another. For initial network turn up, see Chapter 5, "Turn Up Network."

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-154 Upgrade a Point-to-Point to a Linear ADM, page 13-2—Complete as needed.
2. NTP-155 Upgrade a Point-to-Point or a Linear ADM to a Two-Fiber BLSR, page 13-3—Complete as needed.
3. NTP-156 Upgrade a Point-to-Point or Linear ADM to a UPSR, page 13-7—Complete as needed.
4. NTP-157 Upgrade a USPR to a BLSR, page 13-8—Complete as needed.
5. NTP-158 Upgrade a Two-Fiber BLSR to a Four-Fiber BLSR, page 13-10—Complete as needed.
6. NTP-159 Modify a BLSR, page 13-13—Complete as needed.

NTP-154 Upgrade 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 (3 or more nodes).
Tools/Equipment	None
Prerequisite Procedures	The node that will be added must have OC-N cards installed. See Chapter 2, "Install Cards and Fiber-Optic Cable," and Chapter 4, "Turn Up Node," for procedures.
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 2-3 on page 2-22.

Note In a point-to-point configuration, two OC-N cards are connected to two OC-N cards on a second node. Any multispeed slot (OC-3, OC-12, OC12-4, OC48AS cards only) or high-speed slot (any OC-N card except the OC12-4) can be used if connections between nodes are consistent. For example, Slot 5 on the first point-to-point node connects to Slot 5 on the second point-to-point node for the working path, and Slot 6 connects to Slot 6 for the protect path. The OC-N ports have DCC terminations, and the OC-N cards are in a 1+1 protection group.

Step 1 Log into a point-to-point node. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Check the point-to-point network for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all point-to-point spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD.

c. Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no switches are active.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Log into the node that will be added to the point-to-point configuration.

Step 4 Complete the "NTP-24 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-35 Verify Node Turn Up" procedure on page 5-2 for the new node.

Step 6 Physically connect the fibers between the point-to-point node and the new node.

Step 7 On the new node, create a 1+1 protection group for the OC-N cards that will connect to the point-to-point node. See the "DLP-73 Create a 1+1 Protection Group" task on page 4-27 for instructions.

Step 8 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 for the OC-N cards in the new node that will connect to the linear ADM network. Make sure to set Port State on the Create SDCC Termination dialog box to IS.

Note DCC failure alarms display until you create DCC terminations in the point-to-point node.

Step 9 Display the point-to-point node that will connect to the new node in CTC node view.

Step 10 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-73 Create a 1+1 Protection Group" task on page 4-27 for instructions.

Step 12 Create DCC terminations on the OC-N cards that will connect to the new node. See the "DLP-213 Provision SONET DCC Terminations" task on page 5-4. On the Create SDCC Termination dialog box, set the port state to IS.

Step 13 Display the new node in node view.

Step 14 Complete the "NTP-28 Set Up Timing" task on page 4-18 for the new node. If the new node is using line timing, set the working OC-N card as the timing source.

Step 15 Display the network view to verify that the newly-created linear ADM configuration is correct. Two green span lines should display between each linear node.

Step 16 Click the **Alarms** tab. Verify that there are no unexpected alarms are displayed.

Step 17 Repeat the procedure to add an additional node to the linear ADM.

NTP-155 Upgrade a Point-to-Point or a Linear ADM to a Two-Fiber BLSR

Purpose	This procedure upgrades a point-to-point configuration or linear ADM to a two-fiber BLSR.
Tools/Equipment	None
Prerequisite Procedures	None
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 the specifications section for each card in the *Cisco ONS 15454 Reference Manual*.

Step 1 Log into one of the nodes that you want to upgrade from a point-to-point or ADM to a BLSR. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 Check for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD.

c. Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no switches are active.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Right-click a span adjacent to the node you are logged into.

Step 4 From the popup window click **Circuits**. The Circuits on Span window appears.

Step 5 Verify that the total number of active STS circuits does not exceed 50% of the span bandwidth. In the Circuits column there is a block titled “Unused”— this number should not exceed 50% 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.

Warning **If the 50% capacity is exceeded this procedure cannot be completed. Bandwidth must be 50% unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.**

Step 6 Repeat Step 3 through Step 5 for each node in the point-to-point or linear ADM that you will convert to BLSR. If all nodes comply with Step 5, proceed to Step 7.

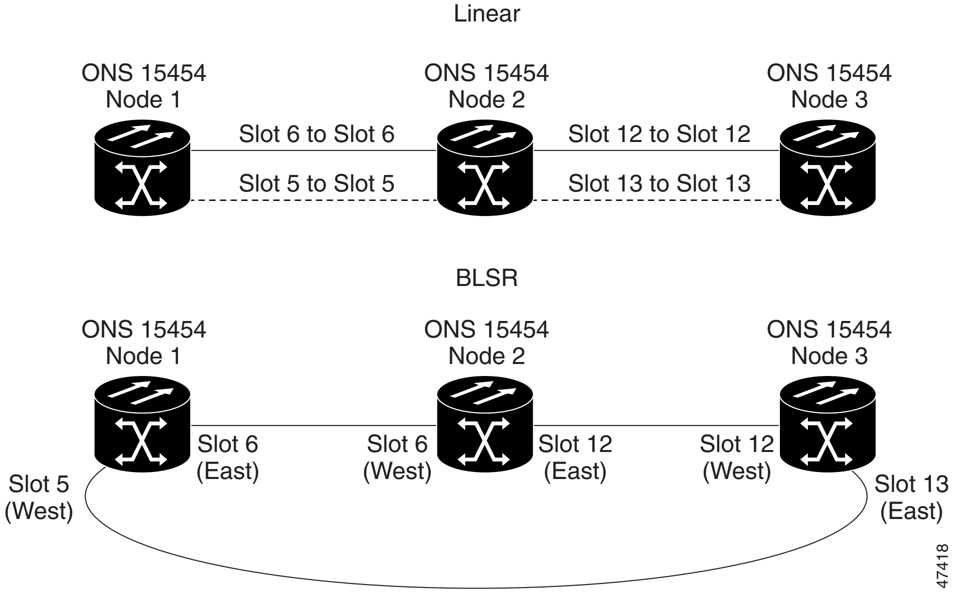
Step 7 Complete the “DLP-189 Verify that a 1+1 Working Slot is Active” task on page 13-6 for every 1+1 protection group that supports a span in the point-to-point or linear ADM network.

Step 8 Complete the “DLP-155 Delete a Protection Group” task on page 10-18 at each node that supports the point-to-point or linear ADM span.

Step 9 Complete the “DLP-214 Change the Service State for a Port” task on page 5-5 to put the protect ports out of service at each node that supports the linear ADM span.

Step 10 (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 13-1) can be removed.

Figure 13-1 Linear ADM to BLSR upgrade



Step 11 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 13-1) can be rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

Note If you need to physically remove any OC-N cards, do so now. In this example, cards in Node 2/Slots 5 and 13 can be removed. See the "NTP-116 Remove and Replace a Card" procedure on page 2-18.

Step 12 From the network view, click the **Circuits** tabs and complete the "DLP-139 Export CTC Data" task on page 7-3 to save the circuit data to a file on your hard drive.

Step 13 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 at the end nodes; provision the slot in each node that is not already in the SDCC Terminations list (in the Figure 13-1 example, Port 1 of Node 1/Slot 5 and Port 1 of Node 3/Slot 13).

Step 14 For circuits provisioned on an STS that is now part of the protection bandwidth (STSs 7–12 for an OC-12 BLSR, STSs 25–48 for an OC-48 BLSR, and 97-192 for an OC-192), delete and recreate each circuit:

a. Complete the "NTP-152 Delete Circuits" procedure on page 9-11 for one circuit.

b. Create the circuit on STSs 1–6 for an OC-12 BLSR, 1–24 for an OC-48 BLSR, or 1–96 for an OC-192 BLSR on the fiber that served as the protect fiber in the linear ADM. See the "NTP-137 Create a Manually Routed Optical Circuit" procedure on page 6-41 for instructions.

c. Repeat Steps a–b for each circuit residing on a BLSR protect STS.

Note Deleting circuits is service affecting.

Step 15 Complete the "NTP-126 Create a BLSR" task on page 5-19 to put the nodes into a BLSR.

DLP-189 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-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Both

Step 1 In the node view, click the **Maintenance > Protection** tabs.

Step 2 Under Selected Group, 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, manually switch traffic to the working slot:

a. Under Selected Group choose the Protect/Active slot.

a. In Switch Commands, choose **Manual**.

b. Click **Yes** on 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 may 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 Switch Commands, choose **Clear**.

b. Click **Yes** on the confirmation dialog box.

Step 6 Return to your originating procedure (NTP).

NTP-156 Upgrade a Point-to-Point or Linear ADM to a UPSR

Purpose	This procedure upgrades a point-to-point system to a UPSR.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits will be deleted and reprovisioned.

Step 1 Log into a node on the point-to-point or linear ADM. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Check for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD.

c. Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no switches are active.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 7, "Manage Alarms," or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Complete the "DLP-189 Verify that a 1+1 Working Slot is Active" task on page 13-6 for each node.

Step 4 Complete the "DLP-155 Delete a Protection Group" task on page 10-18 for each 1+1 protection group that supports the point-to-point or linear ADM span.

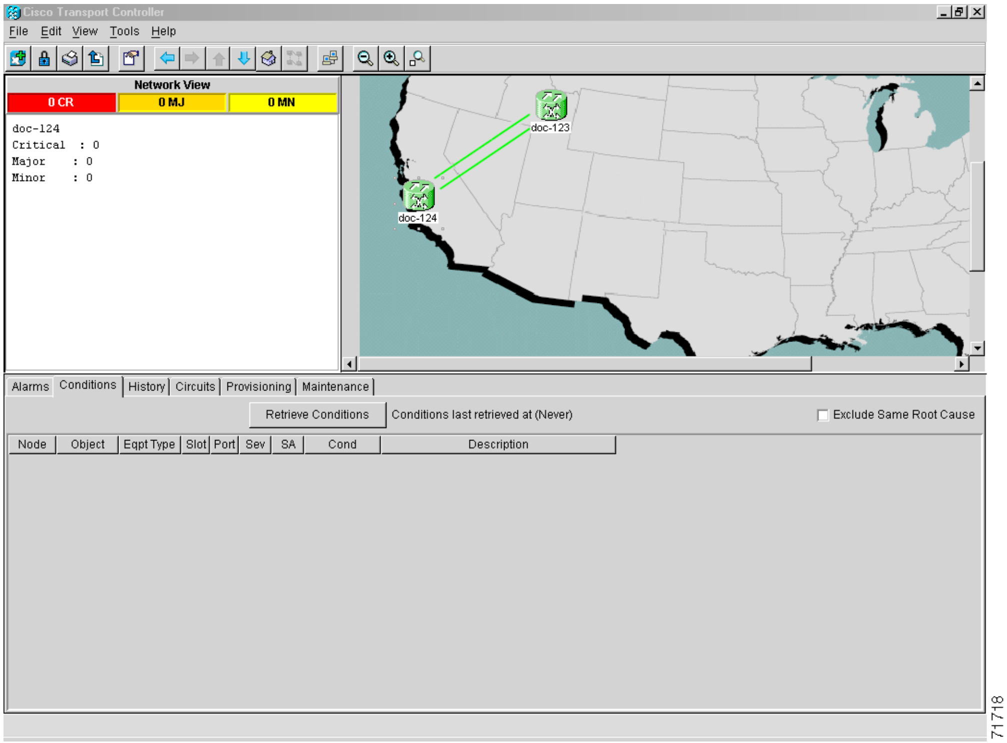
Step 5 Complete the "DLP-213 Provision SONET DCC Terminations" task on page 5-4 at the protect cards in all nodes.

Step 6 Complete the "NTP-152 Delete Circuits" procedure on page 9-11 and the "NTP-136 Create an Automatically Routed Optical Circuit" procedure on page 6-38 to delete and recreate the circuits one at a time.

Note Deleting circuits is service affecting.

Step 7 At the network view verify that the newly-created ring is correct (Figure 13-2).

Figure 13-2 CTC network view with a two-node UPSR



```
doc-124
Critical  : 0
Major     : 0
Minor     : 0
```

NTP-157 Upgrade a USPR to a BLSR

Purpose	This procedure upgrades a UPSR to a BLSR.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits on the ring will be deleted and re-provisioned.

Caution Read through this procedure completely before beginning the upgrade.

Note Prior to beginning this procedure you should have a unique Ring ID number to identify the new BLSR and a unique Node ID number for each node on the ring.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15454 Reference Manual*.

Step 1 Log into an ONS 15454 on the network where you will begin the ring conversion. See the "DLP-60 Log into CTC" task on page 3-22.

Step 2 Check for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD.

c. Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no switches are active.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 7, "Manage Alarms," or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 3 Click **View > Go to Network View**.

Step 4 Right-click a span adjacent to the node you are logged into.

Step 5 From the popup window click **Circuits**. The Circuits on Span window appears.

Step 6 Verify that the total number of active STS circuits does not exceed 50% of the span bandwidth. In the Circuits column there is a block titled "Unused," this number should not exceed 50% 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.

Warning **If the 50% capacity is exceeded this procedure cannot be completed. Bandwidth must be 50% unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.**

Step 7 Repeat Step 1–6 for each node in the UPSR that you will convert to BLSR. If all nodes comply with Step 6, proceed to Step 8.

Step 8 Save all circuit information:

a. In network view, click the **Provisioning > Circuits** tabs.

b. Record the circuit information using one of the following tasks:

- From the File menu, click **Print** to print the circuits table, or
- From the File menu, click **Export** to export the circuit data in HTML, CSV (comma separated values), or TSV (tab separated values). Click **Ok** and save the file in a temporary directory.

  See the "NTP-80 Document Existing Provisioning" procedure on page 7-2 for more information.

Step 9 Delete the circuits:

Note This method uses the network view. To delete circuits one at a time from each node, see the "NTP-152 Delete Circuits" procedure on page 9-11.

a. From network view click the **Circuits** tab. All circuits on the ring will display.

b. With the **Shift** key pressed, left-click each circuit in the display. Each line in the display will turn dark blue as it is selected.

c. After all circuits have been selected click the **Delete** button. Allow several minutes for processing; the actual length of time will depend on the number of circuits in the network.

Step 10 Complete the "NTP-126 Create a BLSR" procedure on page 5-19 to create the BLSR.

Step 11 Complete the "NTP-42 Two-Fiber BLSR Acceptance Test" procedure on page 5-21.

Step 12 To recreate the circuits, see Chapter 6, "Create Circuits and VT Tunnels" and choose the applicable procedure for the circuit type you want to enter.

NTP-158 Upgrade a Two-Fiber BLSR to a Four-Fiber BLSR

Purpose	This procedure upgrades a two-fiber BLSR to a four-fiber BLSR.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Two-fiber OC-48 or OC-192 BLSRs can be upgraded to four-fiber BLSRs. To upgrade, you install two additional OC-48 or OC-192 cards at each two-fiber BLSR node, then log into CTC and upgrade 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.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15454 Reference Manual*.

Step 1 Complete the "DLP-60 Log into CTC" task on page 3-22 to log into one of the two-fiber nodes that you want to upgrade.

Step 2 Check the BLSR for outstanding alarms and conditions:

a. From the View menu, choose **Go to Network View**.

b. Verify that all spans between BLSR nodes on the network map are green.

c. 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. In a BLSR, these facility conditions may be reported as minor alarms.

d. Click the **Conditions** tab, then click **Retrieve Conditions**. Verify that no ring switches are active.

If trouble is indicated, for example, a major alarm exists, resolve the problem before proceeding to Step 3. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information about alarms.

Step 3 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. See Chapter 2, "Install Cards and Fiber-Optic Cable," for installation procedures.

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.

Step 5 Complete the "DLP-214 Change the Service State for a Port" procedure on page 5-5 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 Upgrade the BLSR:

a. Display the network view and click the **Provisioning > BLSR** tabs.

b. Choose the two-fiber BLSR you want to upgrade then click the **Upgrade to 4 Fiber** button.

c. On the Upgrade BLSR dialog box, 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.

d. Click **Next**.

e. Assign the east and west protection ports:

   - *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.

f. Click **Finish**.

Step 8 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 an alarm is present, resolve the problem before proceeding to the next step. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information about alarms.

Step 9 Test the four-fiber BLSR. See the "NTP-43 Four-Fiber BLSR Acceptance Test" procedure on page 5-26.

DLP-238 Initiate a BLSR Span Lockout

Purpose	Use this task to perform a BLSR span lockout, which prevents traffic from switching to the locked out span.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a span lockout.

Step 1 Display the 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 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 To lock out a west span:

a. Right-click any BLSR node west port and choose **Set West Protection Operation**. Figure 13-3 shows an example.

> **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.

Figure 13-3 Invoking a protection operation on a three-node BLSR

b. On the Set West Protection Operation dialog box, choose **LOCKOUT SPAN** from the drop-down menu. Click **OK**.

c. On the Confirm BLSR Operation dialog box, click **Yes**.

Step 5 To lock out an east span:

a. Right-click the node's east port and choose **Set East Protection Operation**.

b. On the Set East Protection Operation dialog box, choose **LOCKOUT SPAN** from the drop-down menu. Click **OK**.

c. On the Confirm BLSR Operation dialog box, click **Yes**.

On the network graphic, an L is displayed on the working BLSR channel where you invoked the protection switch.

Performing a lockout switch generates LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-239 Clear a BLSR Span Lockout

Purpose	Use this task to clear a BLSR span lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a force protection switch.

Step 1 Display the 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 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 port where the lockout will be cleared and choose **Set West Protection Operation** or **Set East Protection**.

Step 5 On the dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 6 On the Confirm BLSR Operation dialog box, click **Yes**.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

NTP-159 Modify a BLSR

Purpose	Use this procedure to change a BLSR ring ID, node ID, and ring and span reversion times.
Tools/Equipment	None
Prerequisite Procedures	"NTP-126 Create a BLSR" procedure on page 5-19
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Some or all of the following alarms display during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR. For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 1 Log into a node in the BLSR you want to modify. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 To change the BLSR ring ID or the ring or span reversion times, complete the following steps. If you want to change a node ID, go to Step 4.

a. Switch to network view and click the **Provisioning > BLSR** tabs.

b. Click the BLSR you want to modify and click **Edit**.

c. On the BLSR window, change any of the following:

- *Ring ID*—If needed, change the BLSR ring ID (a number between 0 and 9999).
- *Reversion time*—If needed, change the amount of time that will pass before the traffic reverts to the original working path following a ring switch.
- *Span Reversion*—(4 Fiber BLSRs only) If needed, change the amount of time that will pass before the traffic reverts to the original working path following a span switch.

d. Click **Apply**.

If you changed the ring ID, the BLSR window closes automatically. If you only changed a reversion time, close the window by choosing **Close** from the window File menu.

Step 3 To change a BLSR node ID, complete the following steps; otherwise, proceed to Step 4.

a. On the network map, double-click the node with the node ID you want to change.

b. Click the **Provisioning > BLSR** tabs.

c. Choose the Node ID. Do not choose a number already assigned to another BLSR.

d. Click **Apply**.

Step 4 Switch to network view and 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

Note For definitions of these alarms, see the *Cisco ONS 15454 Troubleshooting Guide*.

Step 5 Initiate a manual ring switch on the BLSR to verify traffic switches normally. See the "DLP-240 Initiate a BLSR Manual Ring Switch" task on page 13-15. If it does, go to the next step. If not, begin troubleshooting to see why the switch did not occur.

Step 6 Complete the "DLP-241 Clear a BLSR Manual Ring Switch" task on page 13-16.

Step 7 Repeat Steps 5 – 6 on each node in the network.

Step 8 Disconnect the fibers at one node and verify that traffic switches normally. If traffic does not switch, complete the "NTP-112 Clean Fiber Connectors" procedure on page 15-21 and reconnect the fibers.

DLP-240 Initiate a BLSR Manual Ring Switch

Purpose	Use this task to perform a BLSR manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a force protection switch.

Step 1 Display the 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 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 any BLSR node port and choose **Set West Protection Operation** (if you chose a west port) or **Set East Protection Operation** (if you chose an east port).

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.

Step 5 On the Set West Protection Operation dialog box or the Set East Protection dialog box, choose **LOCKOUT SPAN** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** on the two Confirm BLSR Operation dialog boxes.

Step 7 Verify that the span lines between the nodes where the manual switch was invoked turn purple, and span lines between all other nodes turn green. This confirms the manual switch.

Step 8 From the File menu, choose **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-241 Clear a BLSR Manual Ring Switch

Purpose	Use this task to clear a manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a force protection switch.

Step 1 Display the 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 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 port where the manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 On the dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** on the Confirm BLSR Operation dialog box.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

Add and Remove Nodes

This chapter explains how to add and remove nodes by forcing a protection switch to route traffic away from the span where you will add or remove the node.

Before You Begin

Before performing any of the following procedures, complete the "NTP-80 Document Existing Provisioning" procedure on page 7-2. 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-160 Add a BLSR Node, page 14-2—Complete as needed.
2. NTP-161 Remove a BLSR Node, page 14-10—Complete as needed.
3. NTP-105 Add a UPSR Node, page 14-14—Complete as needed.
4. NTP-106 Remove a UPSR Node, page 14-16—Complete as needed.

NTP-160 Add a BLSR Node

Purpose	Use this procedure to expand a BLSR by adding a node.
Tools/Equipment	Fiber for new node connections
Prerequisite Procedures	Cards must be installed and node turnup 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 line cards that will connect to the new node. (The line cards are where the BLSR DCC terminations are created.) This information is essential to complete this procedure without error. Figure 14-1 and Figure 14-2 show an example.

Note The example uses Slots 5 and 12 as the west and east lines. However, you can use any OC-N slot as long as you use the same slots consistently throughout the BLSR to prevent fiber connection errors from occurring.

Figure 14-1 A 3-node two-fiber BLSR before a fourth node is added

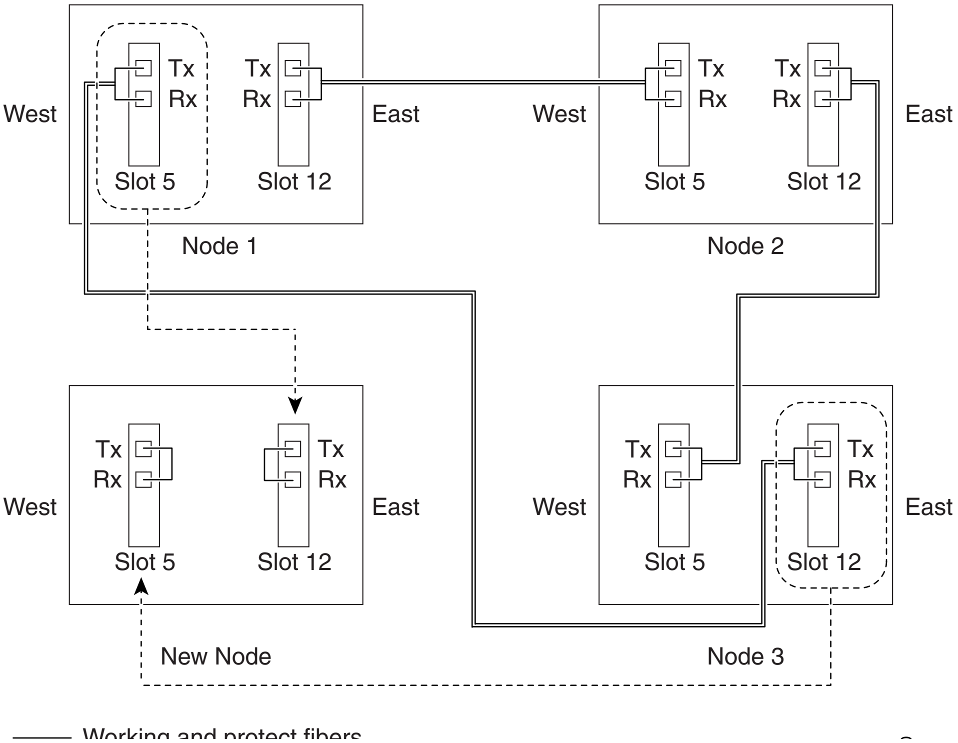
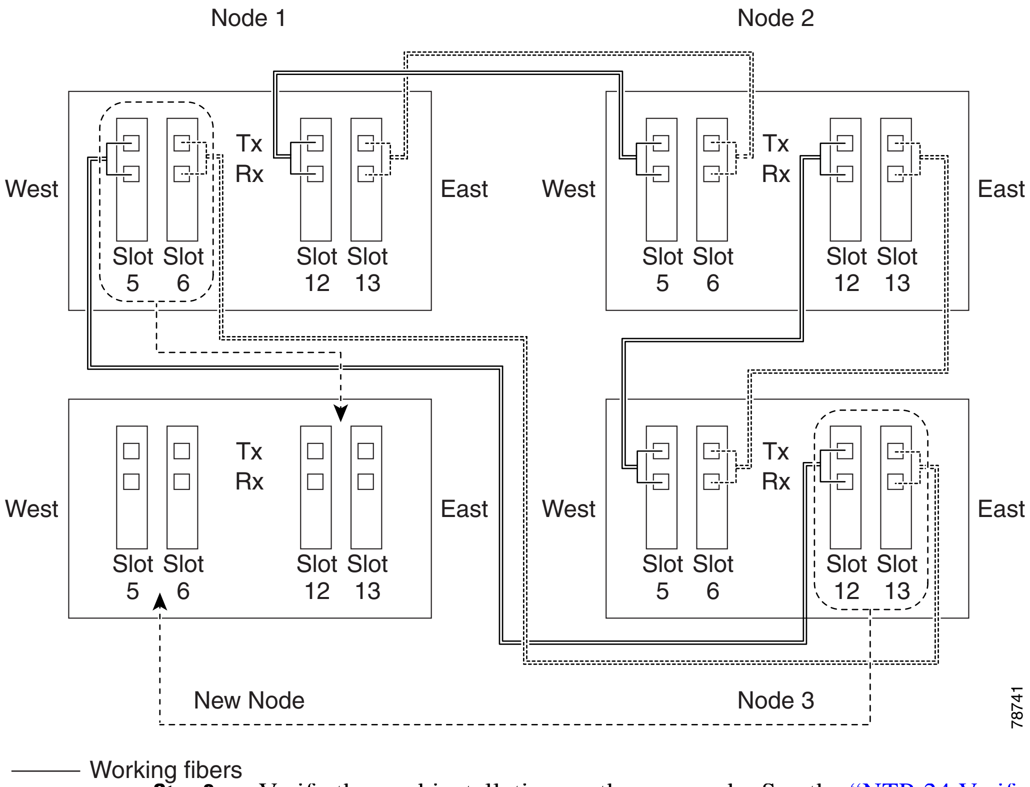


Figure 14-2 A 3-node four-fiber BLSR before a fourth node is added



Step 2 Verify the card installation on the new node. See the “NTP-24 Verify Card Installation” procedure on

page 4-2. Verify that the OC-N cards that will be the BLSR line 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-16 Install the Optical Cards" procedure on page 2-11.

Step 3 Verify that fiber is available to connect the new node to the existing nodes. Refer to the diagram drawn in Step 1.

Step 4 Complete the "NTP-35 Verify Node Turn Up" procedure on page 5-2. 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 5 Check to see if the new node IP address is on the same subnet as other nodes in the network. If two or more PCs are directly connected to different nodes that belong to the same subnet and Craft Access Only is not checked under Gateway Settings, add static routes on the gateway ONS 15454 nodes, using the following settings:

Destination IP address: local PC IP address
Net Mask: 255.255.255.255
Next Hop: IP address of the Cisco ONS 15454
Cost: 1

See the "DLP-65 Create a Static Route" task on page 4-11.

Step 6 Log into a node that is in the BLSR. See the "DLP-60 Log into CTC" task on page 3-22.

Step 7 Check the BLSR for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all BLSR spans on the network map are green.

b. 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. In a BLSR, these facility conditions may be reported as minor alarms. Make sure the Filter button in the lower right corner of window is off (not depressed).

c. Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no ring switches are active. Make sure the Filter button in the lower right corner of window is off.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 7, "Manage Alarms,"or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 8 Click the **Provisioning > BLSR** tabs.

Step 9 On paper, record the Ring ID, Ring Type, Line Rate, Ring Reversion and Span Reversion (4 Fiber).

Step 10 From the Node column, record the Node IDs in the BLSR. The Node IDs are the numbers in parenthesis next to the node name.

Step 11 Log into the new node. If the node has a LAN connection and is displayed 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, you will need to log into it directly. See "DLP-60 Log into CTC" task on page 3-22.

Step 12 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 Chapter 7, "Manage Alarms,"or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 13 Using the information recorded in Steps 9 and 10 and the diagram created in Step 1, create a BLSR on the new node. See the "DLP-242 Create a BLSR on a Single Node" task on page 14-6.

Step 14 (Optional) Create test circuits, making sure they pass through the BLSR line cards, and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-137 Create a Manually Routed Optical Circuit" procedure on page 6-41 and the "NTP-62 Test Optical Circuits" procedure on page 6-50 for information.

Step 15 Create the DCC terminations on the new node. See the "DLP-213 Provision SONET DCC Terminations" task on page 5-4.

Note Creating the DCC terminations will cause SDCC Termination Failure and LOS Loss of Signal alarms to display. These alarms will display 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-89 Remap the K3 Byte" task on page 5-18.

Step 16 Log into a BLSR node that will connect to the new node. See "DLP-60 Log into CTC" task on page 3-22.

Step 17 Referring to the diagram created in Step 1, complete the "DLP-243 Initiate a BLSR Force Ring Switch" task on page 14-7 on the node that will connect to the new node on its west line.

Step 18 Referring to the diagram created in Step 1, complete the "DLP-243 Initiate a BLSR Force Ring Switch" task on page 14-7 on the node that will connect to the new node on its east line.

Step 19 Click the **Alarms** tab. If unexpected critical or major alarms are displayed, resolve them before you continue. If necessary, refer to the Alarm Troubleshooting procedures in the *Cisco ONS 15454 Troubleshooting Guide*.

Step 20 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 14-1 example, this is Node 1/Slot 5, and in Figure 14-2 this is Node 1, Slots 5 and 6.

b. Remove the east fiber from the node that will connect to the east port of the new node. In the Figure 14-1 example, this is Node 3/Slot 12, and in Figure 14-2 this is Node 1, Slots 12 and 13.

Step 21 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 4-fiber BLSRs, connect the protect fibers.

Step 22 Display the newly added node in node view.

Step 23 Click the **Provisioning > BLSR** tabs.

Step 24 Click **Ring Map**. Verify that the new node appears on the Ring Map with the other BLSR nodes, then click **OK**.

Step 25 From the View menu, choose **Go to Network View** and check the following:

a. Click the **Provisioning > BLSR** tabs. Verify that the new node is displayed under Nodes.

b. Click the Alarms tab. Verify that BLSR alarms such as RING MISMATCH, E-W MISMATCH, PRC-DUPID (duplicate node ID) or APSCDFLTK (default K) are not displayed.

If the new node does not appear under Node, or if BLSR alarms are displayed, log into the new node and verify that the BLSR is provisioned on it correctly with the information from Steps 9 and 10. If the node still does not appear, or if alarms persist, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 26 Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node will be shown as incomplete.

Step 27 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 displayed in the dialog box is correct.

Step 28 If incomplete circuits are still displayed refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 29 Click the **History** tab. Verify that BLSR_RESYNC conditions are displayed for every node in the BLSR.

Step 30 Complete the "DLP-194 Clear a BLSR Force Ring Switch" task on page 14-9 to remove the Force Switch from the east and west BLSR lines.

Step 31 (Optional) Complete the "NTP-42 Two-Fiber BLSR Acceptance Test" procedure on page 5-21.

DLP-242 Create a BLSR on a Single Node

Purpose	Use this task to create a BLSR on a single node. The task is used when you add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily from one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Display the node view.

Step 2 Click the **Maintenance > BLSR** tabs.

Step 3 On the Suggestion dialog box, click **OK**.

Step 4 On 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 ID*—Enter the BLSR Ring ID. If the node is being added to a BLSR, use the BLSR ring ID.
- *Node ID*—Enter the Node ID. If the node is being added to a BLSR, use an ID not used by other BLSR nodes.
- *Ring Reversion*—Enter the ring reversion time of the existing BLSR.
- *West Line*—Enter the slot that will connect to the BLSR through the west line.
- *East Line*—Enter the slot that will connect to the existing BLSR through the east line.

If you are adding the node to a four fiber BLSR, complete the following:

- *Span Reversion*—Enter the span reversion time of the existing BLSR.
- *West Line*—Enter the slot that will connect to the second BLSR line through the west line.
- *East Line*—Enter the slot that will connect to the existing BLSR through the east line.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

Note Alarms are displayed and the BLSR will be displayed as Incomplete until the node is connected to other BLSR nodes.

DLP-243 Initiate a BLSR Force Ring Switch

Purpose	Use this task to perform a BLSR force protection operation on a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a force protection switch.

Step 1 Display the 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** (Figure 14-3). (To move a graphic icon, click it, press **Ctrl**, and drag the icon 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 port.

Figure 14-3 Invoking a protection operation on a three-node BLSR

b. On the Set West Protection Operation or Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down menu. Click **OK**.

c. Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed 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, FORCED-REQ-RING, and WKSWPR.

Step 5 To apply a force switch to the east line:

a. Right-click the west BLSR port and choose **Set East Protection Operation**. (To move a graphic icon, click it, press **Ctrl**, and drag the icon 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 port.

b. On the Set East Protection Operation, choose **FORCE RING** from the drop-down menu. Click **OK**.

c. Click **Yes** on the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F is displayed 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, FORCED-REQ-RING, and WKSWPR.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-194 Clear a BLSR Force Ring Switch

Purpose	Use this task to remove a force switch from a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Display the 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 (ports with a force switch applied will be marked with an F) and choose **Set West Protection Operation**. (To move a graphic icon, click it, press **Ctrl**, and drag the icon to a new location.)

b. On the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

c. On the Confirm BLSR Operation dialog box, click **Yes**.

Step 5 To clear a force switch on the west line:

a. Right-click the BLSR east port where you want to clear the protection switch (ports with a force switch applied will be marked with an F) and choose **Set East Protection Operation**.

b. On the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

c. On 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-161 Remove a BLSR Node

Purpose	Use this procedure to remove a node from a BLSR.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

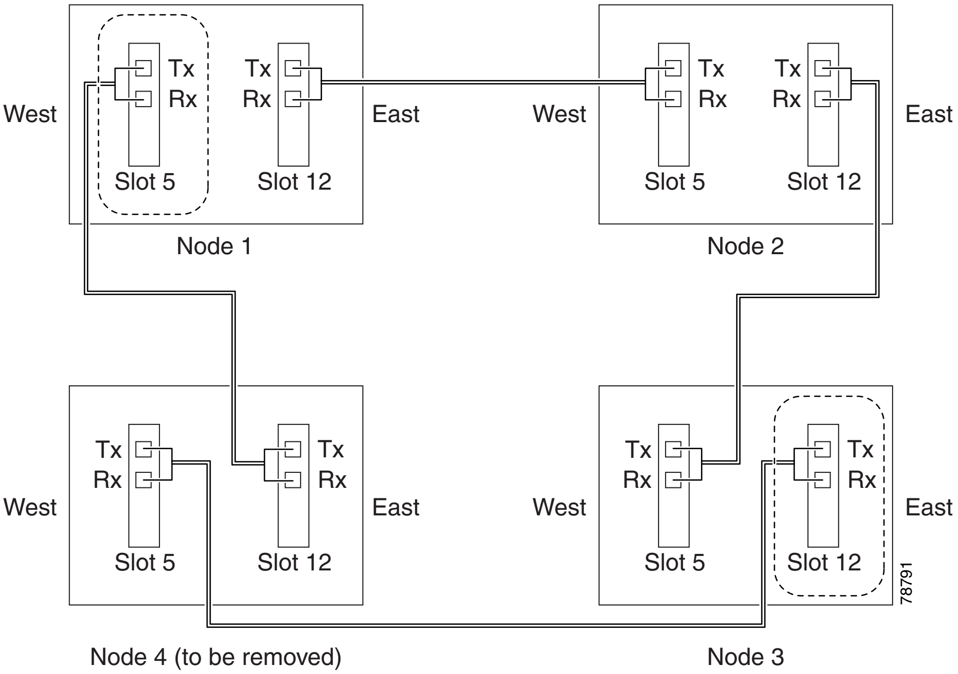
Caution The following procedure minimizes traffic outages during node removals. You will delete all circuits that originate and terminate on the node that will be removed. In addition, if circuits that pass through the node were created with ONS 15454 Release 2.x software, you will verify that they do not enter and exit the node on different STSs. If they do, you will delete and recreate the circuits, and traffic will be lost during this time.

Caution If you remove a node that is the only BITS timing source for the ring, you will 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 Stratum 1 will experience a high level of pointer adjustments, which may adversely affect customer service.

Step 1 Draw a diagram of the BLSR where you will remove the node. In the diagram, identify the following:

- Which node is connected through its west port to the node that will be removed. For example if you were removing Node 4 in Figure 14-4, Node 1 is the node connected through its west port to Node 4.
- Which node is connected through its east port to the node that will be removed. In Figure 14-4, Node 3 is connected to Node 4 through its east port.

Figure 14-4 A 3-node two-fiber BLSR before a node is removed



Step 2 Log into a BLSR node that is not the node that you will remove. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 3 Check the BLSR for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all BLSR spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms. Make sure the Filter button in the lower right corner of window is off (not depressed).

c. Click the **Conditions** tab and click **Retrieve Conditions.** Make sure the Filter button in the lower right corner of window is off (not depressed). Verify that no ring switches are active.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 7, "Manage Alarms"or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 From the View menu, choose **Go to Other Node**. Choose the node that you will remove and click **OK**.

Step 5 Click the **Circuits** tab. If the Scope setting is set to Network, choose **Node** from the Scope drop-down menu. Make sure the Filter button is off to ensure that all circuits are visible.

Step 6 Delete all circuits that originate or terminate on the node. See the "NTP-152 Delete Circuits" procedure on page 9-11.

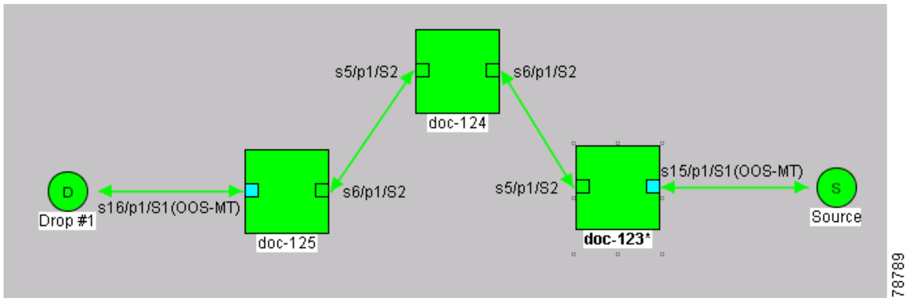
Step 7 Complete this step if any circuits created using ONS 15454 Software Release 2.x pass through the node that will be removed (circuits are displayed on the Circuits tab).

a. Choose a circuit and click **Edit**.

b. On the Edit Circuits window, check **Show Detailed Map**.

c. Verify that the circuits enter and exit the node on the same STS. For example, if a circuit enters on s5/p1/S1 (Slot 5, Port 1, STS 1), verify that it exits on STS 1. If the circuit enters/exits on different STSs, write down the name of the circuit. Figure 14-5 shows a circuit passing through a node, (doc-124) on the same STS, (STS 2).

Figure 14-5 Verifying pass-through STSs



d. Repeat Steps a – c for each circuit displayed on the Circuits tab.

e. Delete, then recreate each circuit recorded in Step c that entered/exited the node on different STSs. To delete the circuit, choose the circuit on the Circuits window, then click the **Delete** button. To create the circuit, see Chapter 6, "Create Circuits and VT Tunnels."

Step 8 From the View menu, choose **Go to Network View**.

Step 9 Referring to the diagram created in Step 1, complete the "DLP-243 Initiate a BLSR Force Ring Switch" task on page 14-7 on the node that connects to the target (removal) node through the target node's west line.

Step 10 Referring to the diagram created in Step 1, complete the "DLP-243 Initiate a BLSR Force Ring Switch" task on page 14-7 on the node that connects to the target (removal) node through the target node's east line.

Step 11 Click the **Alarms** tab. If unexpected critical or major alarms are displayed, resolve them before you continue. If necessary, refer to the Alarm Troubleshooting procedures in the *Cisco ONS 15454 Troubleshooting Guide.*

Step 12 Remove fiber connections between the node being removed and the two neighboring nodes.

Step 13 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Step 14 (Optional) On the removed node, complete the "DLP-196 Delete a BLSR from a Single Node" task on page 14-13 to remove the BLSR from the former BLSR trunk card.

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 15 Click the **History** tab. Verify that the BLSR_RESYNC condition is displayed for every node in the BLSR.

Step 16 Complete the "DLP-194 Clear a BLSR Force Ring Switch" task on page 14-9 to remove the force protection switches.

Step 17 Complete the "DLP-195 Verify Timing in a Reduced Ring" task on page 14-13.

Step 18 (Optional) Complete the "NTP-42 Two-Fiber BLSR Acceptance Test" procedure on page 5-21.

Step 19 Return to your originating procedure (NTP).

DLP-195 Verify Timing in a Reduced Ring

Purpose	Use this task to verify timing in a reduced ring.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite/remote
Security Level	Provisioning or higher

Step 1 Log into the node that you removed from the ring. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 Click the **Provisioning > Timing** tabs.

Step 3 Observe the Timing Mode field to see the type of timing (Line, External, Mixed) that has been set for that node.

Step 4 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 5 If the removed node was the BITS timing source, perform the following:

a. 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-157 Change the Node Timing Source" task on page 10-20.

b. 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 and set the BITS 1 and 2 State to OOS. Then choose line timing for all other nodes in the ring. This will force the first node to be their primary timing source. (See the "DLP-157 Change the Node Timing Source" task on page 10-20.)

Note This type of timing conforms to Stratum 3 requirements and is not considered optimal.

Step 6 If the removed node was not the 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.

Step 7 Return to your originating procedure (NTP).

DLP-196 Delete a BLSR from a Single Node

Caution Use this task only when deleting a BLSR traffic (line) card and traffic has been removed from the line card.

Purpose	Use this task to delete a BLSR from a BLSR trunk card after removing traffic from the card.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning > BLSR** tabs.

Step 2 Highlight the ring and click **Delete**.

Step 3 On the Suggestion dialog box, click **OK**.

Step 4 On the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 5 Return to your originating procedure (NTP).

NTP-105 Add a UPSR Node

Purpose	Use this procedure to add a node to a UPSR.
Tools/Equipment	None
Prerequisite Procedures	Cards must be installed and node turnup procedures completed on the node that will be added to the UPSR. 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

Step 1 Verify the card installation on the new node. See the "NTP-24 Verify Card Installation" procedure on page 4-2. Check that the OC-N cards that will serve as the UPSR line cards match the UPSR optical rate. For example, if the UPSR is OC-48, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the rate does not match the UPSR, complete the "NTP-16 Install the Optical Cards" procedure on page 2-11 to install them.

Step 2 Verify that fiber is available to connect the new node to the existing nodes.

Step 3 Complete the "NTP-35 Verify Node Turn Up" procedure on page 5-2.

Step 4 Log into a node in the network where you want to add a UPSR node. See the "DLP-60 Log into CTC" task on page 3-22 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 5 Check to see if the new node IP address is on the same subnet as other nodes in the network. If two or more PCs are directly connected to different nodes that belong to the same subnet and Craft Access Only is not checked under Gateway Settings, add static routes on the gateway ONS 15454 nodes, using the following settings:

Destination IP address: local PC IP address
Net Mask: 255.255.255.255
Next Hop: IP address of the Cisco ONS 15454
Cost: 1

See the "DLP-65 Create a Static Route" task on page 4-11.

Step 6 Check the UPSR for alarms and conditions:

a. From the View menu, choose **Go to Network View**. Verify that all UPSR spans on the network map are green.

b. Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD. Make sure the Filter button in the lower right corner of window is off (not depressed).

c. Click the **Conditions** tab and click **Retrieve Conditions.** Make sure the Filter button in the lower right corner of window is off (not depressed). Verify that no UPSR switches are active. See the "DLP-198 Clear a UPSR Traffic Switch" task on page 14-19 to clear a UPSR switch.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 7, "Manage Alarms,"or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 7 Log into the new node. If the node has a LAN connection and is displayed 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, you will need to log into it directly. See "DLP-60 Log into CTC" task on page 3-22.

Step 8 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 Chapter 7, "Manage Alarms," or, if necessary, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 9 (Optional) Create test circuits, making sure they pass through the BLSR line cards, and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-137 Create a Manually Routed Optical Circuit" procedure on page 6-41 and the "NTP-62 Test Optical Circuits" procedure on page 6-50 for information.

Step 10 Create the DCC terminations on the new node. See the "DLP-213 Provision SONET DCC Terminations" task on page 5-4.

Step 11 From the View menu, choose **Go to Network View**.

Step 12 Complete the "DLP-197 Switch UPSR Traffic" task on page 14-18 to switch traffic away from the span that will be broken to connect to the new node.

⚠ **Caution** Traffic is not protected during a protection switch.

Step 13 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 14 Replace the removed fibers with fibers connected to the new node.

Step 15 Check to see if your new node's IP address is on the same subnet as other nodes in the network. If two or more PCs are directly connected to different nodes that belong to the same subnet, you need to add static routes on the gateway ONS 15454 nodes, following these rules:

Destination IP address: local PC IP address
Net Mask: 255.255.255.255
Next Hop: IP address of the Cisco ONS 15454
Cost: 1

See the "DLP-65 Create a Static Route" task on page 4-11.

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 UPSR 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.

Step 19 In the network view, right-click the new node and choose **Update Circuits With New Node** from the list of options. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits displayed in the dialog box is correct.

Step 20 Click the **Circuits** tab and verify that no incomplete circuits are displayed.

Step 21 Use the "DLP-198 Clear a UPSR Traffic Switch" task on page 14-19 to clear the protection switch.

Step 22 (Optional) Complete the "NTP-45 UPSR Acceptance Test" procedure on page 5-33.

NTP-106 Remove a UPSR Node

Purpose	Use this procedure to remove a node from a UPSR.
Tools/Equipment	None
Prerequisite Procedures	None
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, if circuits that pass through the node were created with ONS 15454 Release 2.x software, you will verify that they do not enter and exit the node on different STSs. If they do, you will delete and recreate the circuits, and traffic will be lost during this time.

Caution If you remove a node that is the only BITS timing source for the ring, you will remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks which are synchronized to Stratum 1 will experience a high level of pointer adjustments, which may adversely affect customer service.

Step 1 Draw a diagram of the UPSR where you will remove the node. In the diagram, identify the following:

- Which node is connected through its west port to the node that will be removed.
- Which node 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 UPSR node. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 3 From the View menu choose **Go to Network View** to display the UPSR. Verify the following:

- All UPSR spans on the network map are green.
- No critical or major alarms (LOF, LOS, AIS-P, AIS-L) are displayed on the **Alarms** tab. Make sure the Filter button in the lower right corner of window is off (not depressed).
- On the Conditions tab, no UPSR switches are active. See the "DLP-198 Clear a UPSR Traffic Switch" task on page 14-19 to clear any active switches. Make sure the Filter button in the lower right corner of the window is off.

If trouble is indicated (for example, a critical or major alarm exists), resolve the problem before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 4 Complete the "DLP-197 Switch UPSR Traffic" task on page 14-18 for all spans connected to the node you are removing.

⚠ **Caution** Traffic is not protected during a forced protection switch.

Step 5 Complete the "NTP-152 Delete Circuits" procedure on page 9-11 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.)

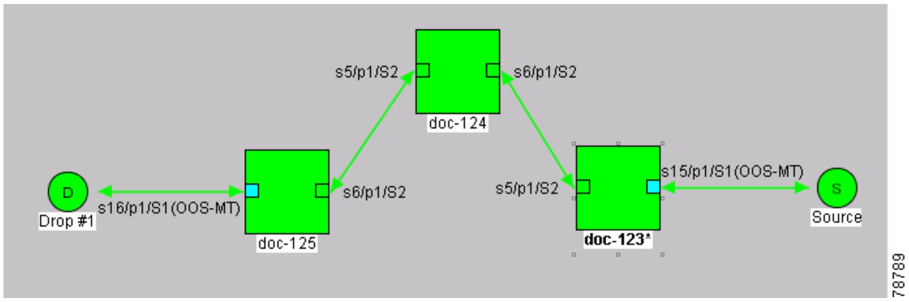
Step 6 Complete this step if any circuits created using ONS 15454 Software Release 2.x pass through the node that will be removed (circuits are displayed on the Circuits tab).

a. Choose a circuit and click **Edit**.

b. On the Edit Circuits window, check **Show Detailed Map**.

c. Verify that circuits enter and exit the node on the same STS. For example, if a circuit enters on s5/p1/S1 (Slot 5, Port 1, STS 1), verify that it exits on STS 1. If the circuit enters/exits on different STSs, write down the name of the circuit. Figure 14-6 shows a circuit passing through a node, (doc-124) on the same STS, (STS 2).

Figure 14-6 Verifying pass-through STSs



d. Repeat Steps a–c for each circuit displayed on the Circuits tab.

e. Delete, then recreate each circuit recorded in Step c that entered/exited the node on different STSs. To delete the circuit, choose the circuit on the Circuits window, then click the **Delete** button. To create the circuit, see Chapter 6, "Create Circuits and VT Tunnels."

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-60 Log into CTC" task on page 3-22 for instructions.

Step 10 Log into the nodes and open the Alarms tab of each newly-connected node. Verify that the span cards are free of alarms. Resolve any alarms before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.

Step 11 See the "NTP-152 Delete Circuits" procedure on page 9-11and Chapter 6, "Create Circuits and VT Tunnels" to delete and recreate each circuit that passed through the deleted node on different STSs.

Step 12 Complete the "DLP-195 Verify Timing in a Reduced Ring" task on page 14-13.

Step 13 Complete the "DLP-198 Clear a UPSR Traffic Switch" task on page 14-19 to clear the protection switch.

Step 14 Click the **Circuits** tab and verify that no incomplete circuits are displayed.

Step 15 (Optional) Complete the "NTP-45 UPSR Acceptance Test" procedure on page 5-33.

DLP-197 Switch UPSR Traffic

Purpose	Use this task to switch UPSR traffic to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Step 1 From the View menu on node view, choose **Go to Network View**.

Step 2 Right-click the span where you want to switch UPSR traffic. Choose **Circuits** from the shortcut menu.

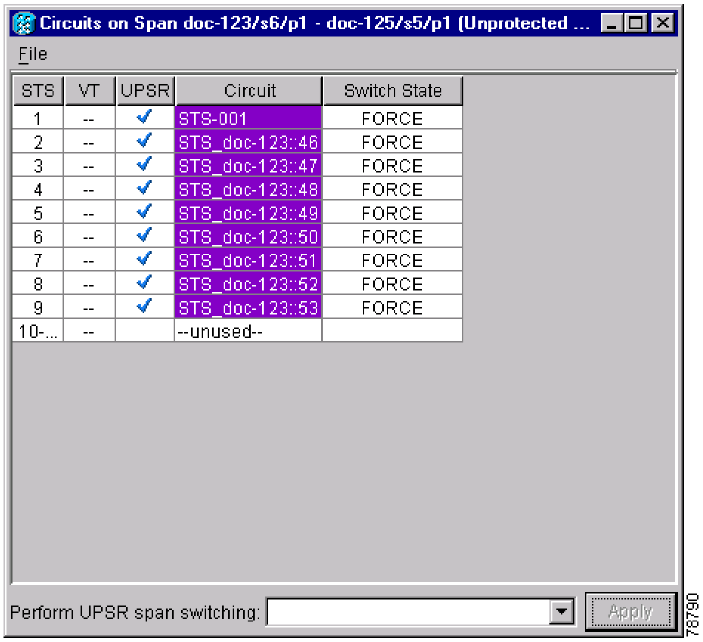
Step 3 On the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 On the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 On the Protection Switch Result dialog box, click **OK**.

On the Circuits on Span window, the Switch State for all circuits is FORCE. Figure 14-7 shows an example.

Figure 14-7 Circuits on Span dialog box with a FORCE switch



Circuits on Span doc-123/s6/p1 - doc-125/s5/p1 (Unprotected ...

STS	VT	UPSR	Circuit	Switch State
1	--	✓	STS-001	FORCE
2	--	✓	STS_doc-123::46	FORCE
3	--	✓	STS_doc-123::47	FORCE
4	--	✓	STS_doc-123::48	FORCE
5	--	✓	STS_doc-123::49	FORCE
6	--	✓	STS_doc-123::50	FORCE
7	--	✓	STS_doc-123::51	FORCE
8	--	✓	STS_doc-123::52	FORCE
9	--	✓	STS_doc-123::53	FORCE
10-...	--		--unused--	

Note A force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition will clear when you clear the force switch; it is informational only.

Step 6 Return to your originating procedure (NTP).

DLP-198 Clear a UPSR Traffic Switch

Purpose	Use this task to clear a previously-issued UPSR traffic switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu on 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 On the Circuits on Span dialog box, choose **CLEAR** to remove a previously-set switch command. Click **Apply**.

Step 4 On the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 On the Protection Switch Result dialog box, click **OK**.

On the Circuits on Span window, the Switch State for all UPSR circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).

CHAPTER 15

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).

1. "NTP-107 Inspect and Maintain the Air Filter" task on page 15-1—Complete as needed.
2. "NTP-108 Back Up the Database" task on page 15-7—Complete as needed.
3. "NTP-109 Restore the Database" task on page 15-8—Complete as needed.
4. "NTP-163 Restore the Node to Factory Configuration" task on page 15-11—Complete as needed to clear the database and upload a blank database and the latest software.
5. "NTP-110 Inhibit Protection Switching" task on page 15-16—Complete as needed.
6. "NTP-111 Revert to an Earlier Software Load" task on page 15-19—Complete as needed
7. "NTP-112 Clean Fiber Connectors" task on page 15-21—Complete as needed.
8. "NTP-113 Reset the TCC+ Using CTC" task on page 15-24—Complete this procedure as needed to reset the TCC+ card and switch the node to the redundant TCC+.

NTP-107 Inspect and Maintain the Air Filter

Purpose	This procedure explains how to inspect and maintain reusable and disposable air filters.
Tools/Equipment	Spare air filters
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

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

Step 1 To maintain the reusable air filter, complete the "DLP-199 Inspect, Clean, and Replace the Reusable Air Filter" task on page 15-2.

Step 2 To maintain the disposable air filter, complete the "DLP-200 Inspect and Replace the Disposable Air Filter" task on page 15-4.

DLP-199 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

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 may have collected on the filter and proceed to Step 9. Figure 15-1 illustrates a reusable fan-tray air filter in an external filter bracket.

Step 3 If the filter is installed beneath the fan tray and not in the external filter brackets, open the front door of the shelf assembly:

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.

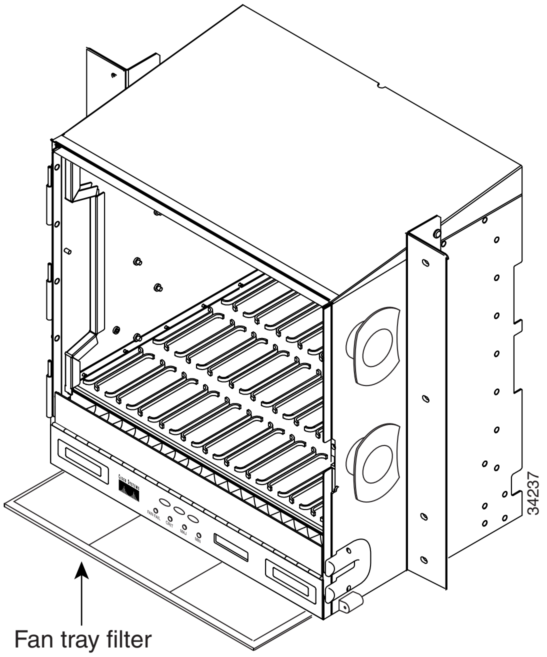
Step 4 Remove the front door (optional). If you do not want to remove the door, proceed to Step 5:

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 15-1 A reusable fan-tray air filter in an external filter bracket (front door removed)



Step 5 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 6 Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.

Step 7 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 8 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that may have collected on the filter.

Step 9 Visually inspect the air filter material for dirt and dust.

Step 10 If the reusable air filter contains a concentration of dirt and dust, replace the dirty air filter with a clean air filter (spare filters should be kept in stock) and re-insert the fan-tray assembly. Then, vacuum or wash the dirty air filter 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 filter:

a. If the air filter is installed in the external filter brackets, slide the dry/clean air filter all the way to the back of the brackets to complete the procedure.

b. If the filter is installed beneath the fan-tray assembly, remove the fan-tray assembly if installed, 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 If applicable, return to your originating procedure (NTP).

DLP-200 Inspect and Replace the Disposable Air Filter

Purpose	This task ensures that the air filter is free from dirt and dust to allow optimum air flow and prevent dirt and dust from entering the ONS 15454.
Tools/Equipment	Extra filters, pinned hex key
Prerequisite Procedures	None
Required/As Needed	Inspection required every 30 days. Replace as needed.
Onsite/Remote	Onsite

Note The disposable air filter is installed beneath the fan-tray assembly only, so you must remove the fan-tray assembly to inspect and replace the disposable air filter.

Step 1 Verify that you are replacing a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. NEBS 3E and earlier versions of the ONS 15454 use a disposable air filter.

Step 2 Open the front door of the shelf assembly.

a. Open the front door lock.

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

b. Press the door button to release the latch.

c. Swing the door open.

Step 3 Remove the front door (optional). If you do not want to remove the door, proceed to Step 4:

a. Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

b. Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

c. Secure the dangling end of the ground strap to the door or chassis with tape.

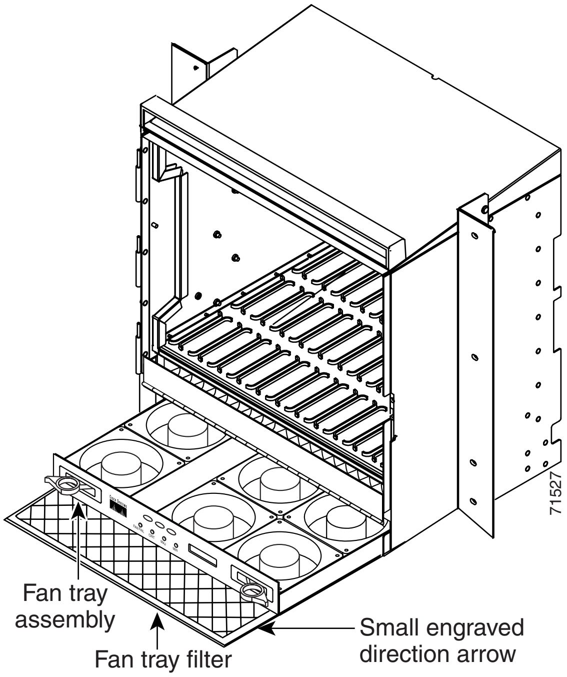
Step 4 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 5 Pull the handles and slide the fan-tray assembly one inch out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 15-2).

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 15-2 Inserting or removing the fan-tray assembly (front door removed)

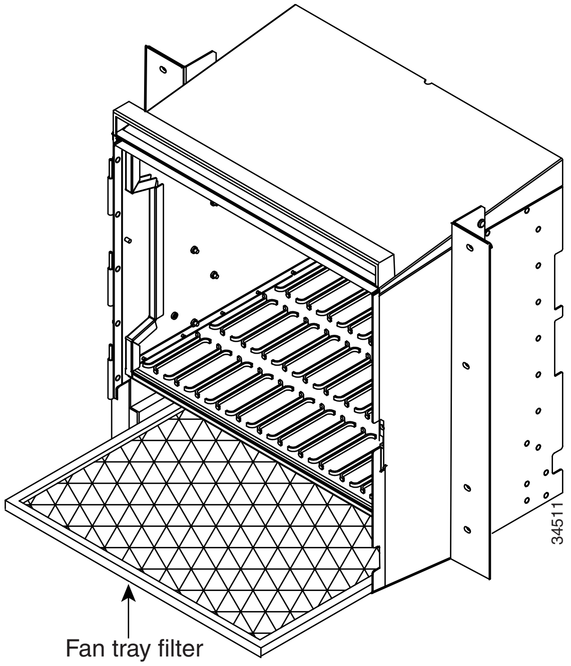


Step 7 Gently remove the air filter from the shelf assembly (Figure 15-3). Be careful not to dislodge any dust that may have collected on the filter.

Step 8 Visually inspect the white filter material for dirt and dust.

Step 9 If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter by sliding the 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 15-3 Inserting or removing a disposable fan-tray air filter (front door removed)



Step 10 Slide the fan-tray assembly into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 11 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 12 Rotate the retractable handles back into their compartments.

Step 13 If you replace the door, also reattach the group strap.

Step 14 Close and lock the door.

Step 15 If applicable, return to your originating procedure (NTP).

NTP-108 Back Up the Database

Purpose	This procedure stores a backup version of the TCC+ (software) database on the workstation running 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	Both
Security Level	Superuser

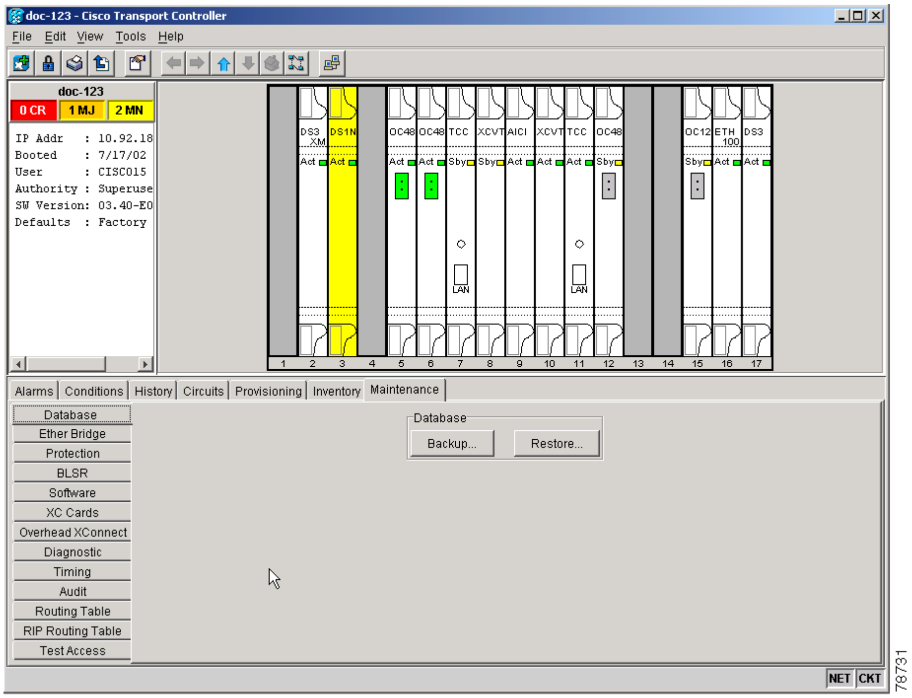
Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

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

Step 1 Log into the node where you will perform the database backup. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22. If you are already logged in, proceed to Step 2.

Step 2 In node (default) view, click the **Maintenance > Database** tabs (Figure 15-4).

Figure 15-4 Backing up the TCC+ database



doc-123 - Cisco Transport Controller

IP Addr : 10.92.18
Booted : 7/17/02
User : CISCO15
Authority : Superuse
SW Version: 03.40-E0
Defaults : Factory

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.

NTP-109 Restore the Database

Purpose	This procedure restores the TCC+/software database.
Tools/Equipment	None
Prerequisite Procedures	NTP-108 Back Up the Database, page 15-7
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Superuser

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

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

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

Step 1 Log into the node where you will restore the database. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22. If you are already logged in, proceed to Step 2.

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

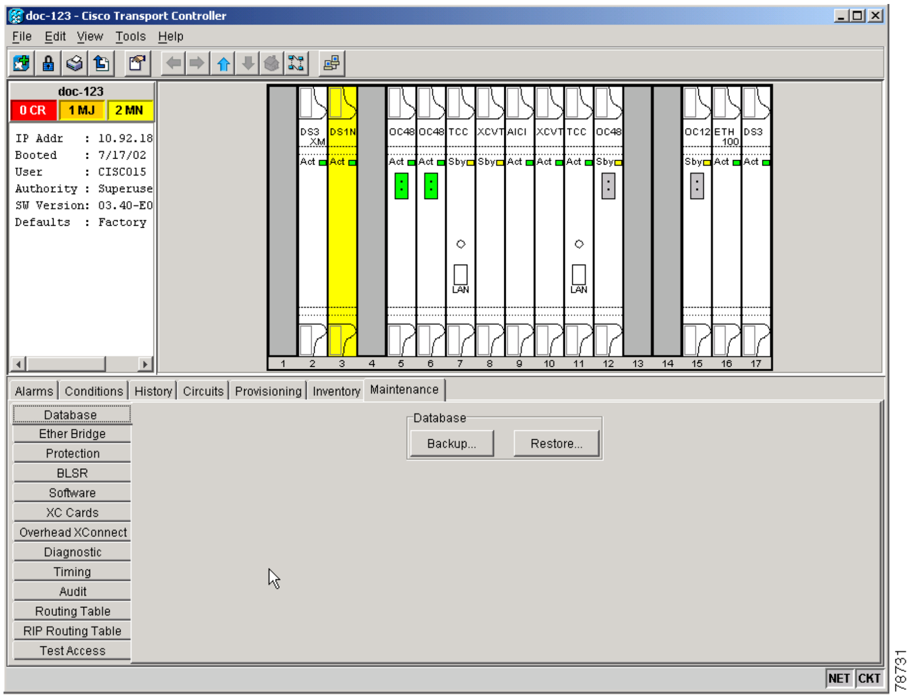
Step 3 If there are switch events that need to be cleared, in node (default) view, click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

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

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

Step 4 In node view, click the **Maintenance > Database** tabs (Figure 15-5).

Figure 15-5 Restoring the TCC+ database



```
IP Addr   : 10.92.18
Booted    : 7/17/02
User      : CISCO15
Authority : Superuse
SW Version: 03.40-E0
Defaults  : Factory
```

Step 5 Click **Restore**.

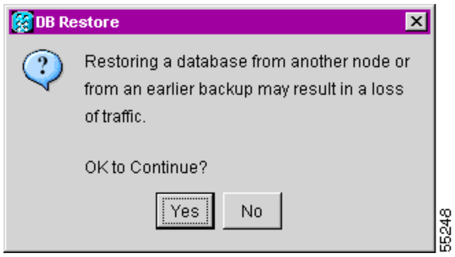
Step 6 Locate the database file stored on the workstation’s hard drive or on network storage.

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 15-6).

Figure 15-6 Restoring the database—traffic loss warning



DB Restore

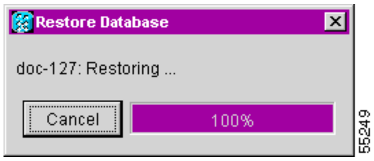
Restoring a database from another node or from an earlier backup may result in a loss of traffic.

OK to Continue?

Step 9 Click **Yes**.

The Restore Database dialog box monitors the file transfer (Figure 15-7).

Figure 15-7 Restoring the database – in-process notification



Restore Database

doc-127: Restoring ...

Step 10 Wait for the file to complete the transfer to the TCC+.

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.

NTP-163 Restore the Node to Factory Configuration

Purpose	Use this procedure to clear the TCC+ database and restore customer or factory defaults. This process involves uploading the most recent software package and a blank database. This process is performed by the RE-INIT.jar utility, also called the reinitialization (reinit) tool.
Tools/Equipment	Software CD containing Release 3.4 software, the node's NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer you will use to perform this procedure.
Prerequisite Procedures	NTP-108 Back Up the Database, page 15-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

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

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

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

Step 1 If you need to install or replace one or more TCC+ cards, see the "DLP-36 Install the TCC+ Cards" task on page 2-6.

Step 2 If you are using Microsoft Windows, complete the "DLP-244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 15-12.

Step 3 If you are using UNIX, complete the "DLP-245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 15-14.

DLP-244 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 TCC+, upload software, and restore factory or customer defaults.
Tools/Equipment	• Software CD containing Release 3.4 software, the NE defaults, and the reinitialization tool • Straight-through (CAT-5) LAN cable
Prerequisite Procedures	NTP-108 Back Up the Database, page 15-7
Required/As Needed	As needed to clear the existing database from a TCC+ and restore the node's default settings.
Onsite/Remote	Onsite
Security Level	Superuser

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

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

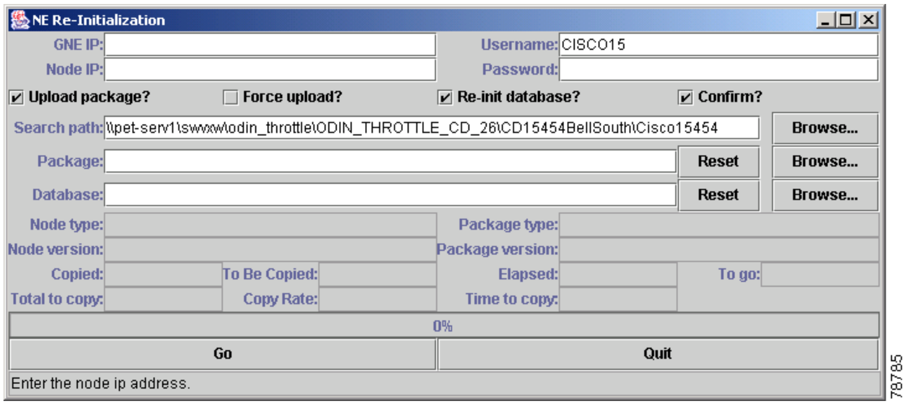
Step 1 Insert the system software CD containing the reinit tool, software, and defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

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

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

Step 4 Select the **RE-INIT.jar** file and click **Open** to open the reinit tool (Figure 15-8).

Figure 15-8 Reinitialization tool in Windows



NE Re-Initialization

GNE IP:
Node IP:
Username: CISCO15
Password:

☑ Upload package? ☐ Force upload? ☑ Re-init database? ☑ Confirm?

Search path: \\pet-serv1\swww\odin_throttle\ODIN_THROTTLE_CD_26\CD15454BellSouth\Cisco15454

Package:
Database:

0%

Enter the node ip address.

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

Step 6 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 15-8).

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

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

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

Step 9 Click **Go**.

Step 10 A confirmation dialog box opens (Figure 15-9). Click **Yes**.

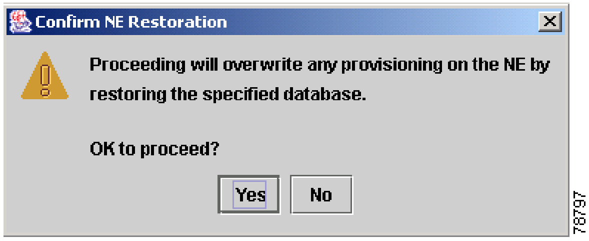
Step 11 The status bar at the bottom of the screen will display Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC+ successfully uploaded the database, not that the database restore was successful. The TCC+ will then try to restore the database after it reboots.

Step 12 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC+ 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. See the "NTP-22 Set Up CTC Computer to Connect to the ONS 15454" procedure on page 3-8.

Step 13 Manually set the node name and network configuration to site-specific values. See the "NTP-25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-3 and "NTP-26 Set Up CTC Network Access" procedure on page 4-5 for information on setting the node name, IP address, mask and gateway, and IIOP port.

Figure 15-9 Confirm NE Restoration



Confirm NE Restoration

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

OK to proceed?

DLP-245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This procedure describes how to use the reinitialization tool in a UNIX environment. Use this tool to clear the database on the TCC+ and restore factory or customer defaults.
Tools/Equipment	Software CD containing Release 3.4 software, the node's NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer you will use to perform this procedure.
Prerequisite Procedures	NTP-108 Back Up the Database, page 15-7
Required/As Needed	As needed to clear the existing database from a TCC+ and restore the node's default settings.
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

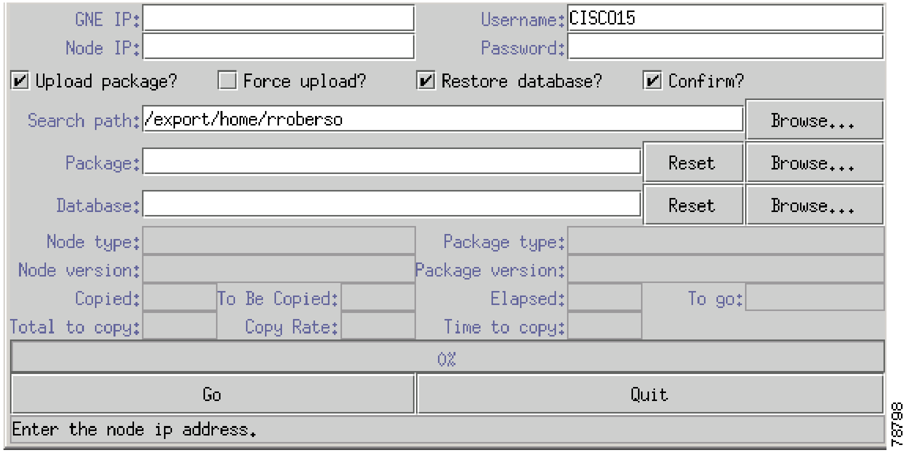
Note The TCC+ cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

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

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

Step 3 If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinit tool (Figure 15-10). If you are working with a command line interface, run *`java -jar RE-INIT.jar`*.

Figure 15-10 The reinitialization tool in UNIX



Username: CISCO15

☑ Upload package? □ Force upload? ☑ Restore database? ☑ Confirm?

Search path: /export/home/rroberso

0%

Enter the node ip address.

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 15-10).

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

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

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

Step 8 Click **Go**.

Step 9 A confirmation dialog box opens (Figure 15-9 on page 15-13). Click **Yes.**

Step 10 The status bar at the bottom of the screen will display Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the TCC+ successfully uploaded the database, not that the database restore was successful. The TCC+ will then try to restore the database after it reboots.

Step 11 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the TCC+ 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. See the "DLP-53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15454" task on page 3-17.

Step 12 Manually set the node name and network configuration to site-specific values. See the "NTP-25 Set Up Name, Date, Time, and Contact Information" procedure on page 4-3 and "NTP-26 Set Up CTC Network Access" procedure on page 4-5 for information on setting the node name, IP address, mask and gateway, and IIOP port.

NTP-110 Inhibit Protection Switching

Purpose	This procedure describes how to apply and remove a Lock On or Lock Out on a traffic card in a protection configuration. For BLSR span lockouts, see "DLP-238 Initiate a BLSR Span Lockout" task on page 13-11 and the "DLP-239 Clear a BLSR Span Lockout" task on page 13-13.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 To prevent traffic on a working or protect card from switching to the other card in the pair, complete the "DLP-201 Apply a Lock On" task on page 15-17.

Step 2 To switch traffic from a working or protect card to the other card in the pair to prevent revertive switching, complete the "DLP-202 Apply a Lock Out" task on page 15-18.

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 3 To remove a Lock On or Lock Out and return a protection group to its usual switching method, complete the "DLP-203 Clear a Lock On or Lock Out" task on page 15-19.

Note A non-alarmed event (INHSW) is raised when a card is placed in a Lock On or Lock Out state.

Note Refer to the *Cisco ONS 15454 Reference Guide* for a description of protection switching and switch state priorities.

DLP-201 Apply a Lock On

Purpose	This task prevents traffic from being switched from one card to another.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance

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 5). When the protect card is active, you can apply the Lock On.

Step 1 Use the following rules to determine if you can put the intended card in a Lock On state:

- For a 1:1 electrical protection group, both the working and protect cards can be placed in the Lock On state.
- For a 1:N electrical protection group, both the working and protect cards can be placed in the Lock On state.
- For a 1+1 optical protection group, only the working card can be placed in the Lock On state.

Step 2 Log into the node where you will apply the Lock On. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 3.

Step 3 In node (default) view, click the **Maintenance > Protection** tabs.

Step 4 Under Protection Groups, click the protection group where you want to apply a lock on.

Step 5 If you determine that the protect card is in standby and you want to apply the lock on to the protect card, make the protect card active:

a. Under Selected Group, click the protect card.

b. Under switch Commands, click **Switch**.

Step 6 Under Selected Group, click the active card where you want to lock traffic.

Step 7 From Inhibit Switching, click **Lock On**.

Step 8 Click **Yes** on 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-203 Clear a Lock On or Lock Out" task on page 15-19.

Step 9 If applicable, return to your originating procedure (NTP).

DLP-202 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 manual switching connections (force, manual, and exercise).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance

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, both the working and protect cards can be placed in the Lock Out state.
- For a 1:N electrical protection group, both the working and protect cards can be placed in the Lock Out state.
- For a 1+1 optical protection group, only the protect card can be placed in the Lock Out state.

Step 2 Log into the node where you will apply the Lock Out. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22. If you are already logged in, go to Step 3.

Step 3 In Node view, click the **Maintenance > Protection** tabs.

Step 4 Under Protection Groups, click the protection group that contains the card you want to lock out.

Step 5 Under Selected Group, click the card you want to lock traffic out of.

Step 6 From Inhibit Switching, click **Lock Out**.

Step 7 Click **Yes** on 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-203 Clear a Lock On or Lock Out" task on page 15-19.

Note Provisioning a lock out causes a LOCKOUT-REQ or an FE-LOCKOUT condition to be raised on CTC. Clearing the lockout switch request clears these conditions; they are informational only.

Step 8 If applicable, return to your originating procedure (NTP).

DLP-203 Clear a Lock On or Lock Out

Purpose	This task clears a lock on or lock out.
Tools/Equipment	None
Prerequisite Procedures	DLP-201 Apply a Lock On, page 15-17 or DLP-202 Apply a Lock Out, page 15-18
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance

Step 1 Log into the node where you will clear the Lock Out or Lock On. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22. If you are already logged in, go to Step 2.

Step 2 In node (default) view, click the **Maintenance > Protection** tabs.

Step 3 Under Protection Groups, click the protection group that contains the card you want to clear.

Step 4 Under Selected Group, click the card you want to clear.

Step 5 From Inhibit Switching, click **Unlock**.

Step 6 Click **Yes** on the confirmation dialog box.

The Lock On or Lock Out is cleared.

Step 7 If applicable, return to your originating procedure (NTP).

NTP-111 Revert to an Earlier Software Load

Prior to Software Release 2.2.1, the ONS 15454 could not revert to an earlier software database without deleting the current database and losing both cross-connect and DCC connectivity. The revert would result in a loss of traffic until the user manually restored the previous database or recreated the existing circuits and provisioning.

Reverting to a 2.2.1 or later load will switch to the older software load and its attendant database without affecting traffic or DCC connectivity. This feature requires dual TCC+ cards and CTC Software R 2.2.1 or later as the protect version.

When you click the Activate button after a software upgrade, the TCC+ copies the current working database and saves it in a reserved location in the TCC+ flash memory. If you later need to revert to the original working software load from the protect software load, the saved database installs automatically. You do not need to restore the database manually or recreate circuits.

Purpose	This procedure reverts the ONS 15454 database to an earlier software load.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Both
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 standby software load without losing traffic. When the next maintenance window opens, complete the upgrade and activate the new software load.

Note A revert to a maintenance release software load will use the current active database; therefore, no provisioning is lost. All other reverts do restore the database. (A maintenance release has a three-digit release number, e.g. 2.2.2).

Note Circuits created and 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 after a revert. This note does not apply to maintenance reverts (e.g. 2.2.2 to 2.2.1), because maintenance releases use the same database.

Step 1 Log into the node where you will perform the revert. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22. The node (default) view appears. If you are already logged in, go to Step 2.

Step 2 Record the IP address of that node:

a. The IP address is displayed on the left side in node view or,

b. In node (default) view, click the **Provisioning > Network > General** tabs.

Step 3 If reverting to a previous software release (not a maintenance release) record any new circuits created since the previous software upgrade because these circuits will have to be manually recreated (if needed) once the software reversion has taken place.

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.

Step 6 Click **Revert**. The Revert button activates the protect software load.

Step 7 Click **Yes** on the revert confirmation dialog box. The ONS 15454 reboots and loses the connection to CTC.

Step 8 Wait until the software upgrade finishes. This may 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. For login procedures, see the "DLP-60 Log into CTC" task on page 3-22.

The browser downloads the CTC applet for the standby software load.

Step 12 If needed, recreate the circuits recorded in Step 3. See Chapter 6, "Create Circuits and VT Tunnels" for specific circuit creation procedures.

NTP-112 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

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 will be unused for 30 minutes or more.

Step 3 Complete the "DLP-204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes" task on page 15-22 as necessary.

Step 4 Complete the "DLP-205 Clean Fiber Connectors with Cletop" task on page 15-22 as necessary.

Step 5 Complete the "DLP-206 Clean the Fiber Adapters" task on page 15-23 as necessary.

Caution Do not reuse the optical swabs. Keep unused swabs off of work surfaces.

DLP-204 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

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 pre-moistened 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 1–3.

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 If applicable, return to your originating procedure (NTP).

DLP-205 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

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 1–3.

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 If applicable, return to your originating procedure (NTP).

DLP-206 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

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 If applicable, return to your originating procedure (NTP).

NTP-113 Reset the TCC+ Using CTC

Purpose	This procedure resets the TCC+ card and switches the node to the redundant TCC+.
Tools/Equipment	None
Prerequisite Procedures	None
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 TCC+, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

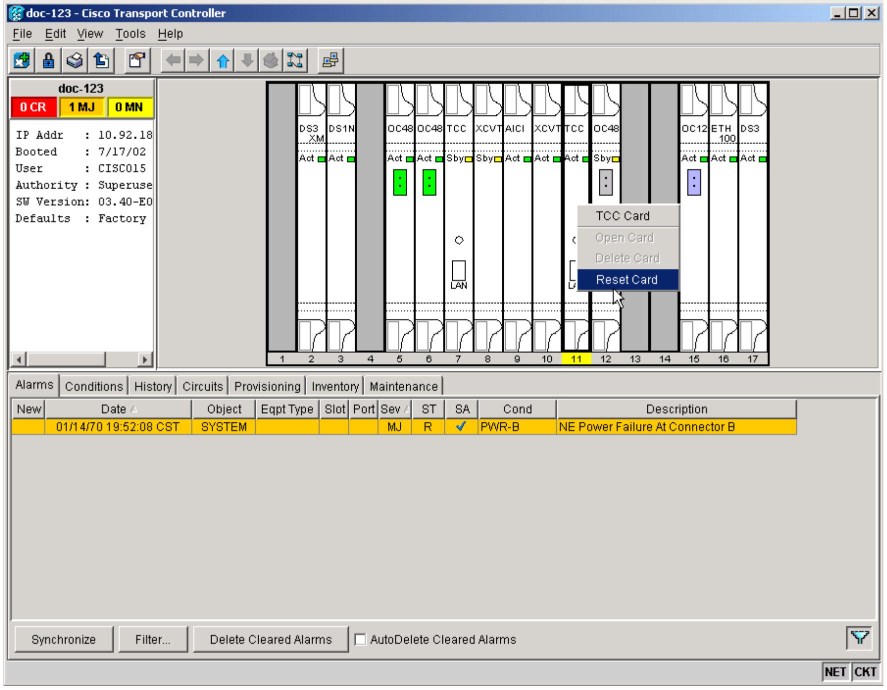
Note When a software reset is performed on an active TCC+, the AIC card goes through an initialization process and also resets. The AIC card reset is normal and will happen each time an active TCC+ card goes through a software-initiated reset.

Step 1 Log into the node where you will perform the software reset. See the "DLP-60 Log into CTC" task on page 3-22 for instructions. If you are already logged in, go to Step 2.

Step 2 In node (default) view, right-click the TCC+ card to reveal a pull-down menu.

Step 3 Click **Reset Card** (Figure 15-11).

Figure 15-11 Performing a software reset from the TCC+ card pull-down menu



```
IP Addr    : 10.92.18
Booted     : 7/17/02
User       : CISCO15
Authority  : Superuse
SW Version: 03.40-E0
Defaults   : Factory
```

New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
	01/14/70 19:52:08 CST	SYSTEM				MJ	R	✓	PWR-B	NE Power Failure At Connector B

□ AutoDelete Cleared Alarms

Step 4 Click **Yes** when the "Are You Sure?" 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 TCC+ reboot, see Table 4-1 on page 4-8.

Step 6 Confirm that the TCC+ you reset is in standby mode after the reset:

a. The TCC+ card's LED will be amber for standby or green for active, or

b. In node view, run the mouse over the TCC+ card and a pop up box will display it the card is active or standby.

CHAPTER 16

Power Down the ONS 15454

This chapter explains how to power down a node and stop all node activity.

Before You Begin

Complete the "NTP-114 Power Down the ONS 15454" procedure on page 16-1 as needed.

NTP-114 Power Down the ONS 15454

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 provision 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 12. If cards are installed, log into the node. See the "DLP-60 Log into CTC" task on page 3-22 for instructions.

Step 2 In network view, 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-161 Remove a BLSR Node" procedure on page 14-10 or the "NTP-160 Add a BLSR Node" procedure on page 14-2. Continue with Step 3.

b. If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 3.

Note Current configurations will be saved if Steps 3–12 are skipped.

Step 3 In node view, click the **Circuits** tab and verify that no circuits are displayed, then proceed to Step 4. 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 4 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 5 In node view, click the **Provisioning > SONET DCC** tabs and delete all SDCC terminations:

a. Click the SDCC Termination that needs to be deleted and click **Delete**.

b. Click **Yes**.

Repeat until no SDCC Terminations are displayed.

Step 6 For each installed 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 7 Remove all fiber connections to the cards.

Step 8 In node view, right-click an installed card and click **Delete**.

Step 9 Click **Yes**.

Step 10 After you have deleted the card, open the card ejectors and remove it from the node.

Step 11 Repeat Step 6–10 for each installed card.

Step 12 Shut off the power from the power supply that feeds the node.

Step 13 Disconnect the node from its external fuse source.

Step 14 Store all the cards you removed and update inventory records according to local site practice.

APPENDIX A

CTC Information and Shortcuts

This appendix describes how to navigate in the Cisco Transport Controller (CTC), change CTC table data display, and export and print data for the Cisco ONS 15454.

Displaying Node, Card, and Network Views

The Cisco Transport Controller provides three views of the ONS 15454 and ONS network:

- Node view displays 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 a map with the ONS 15454 network nodes. 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.

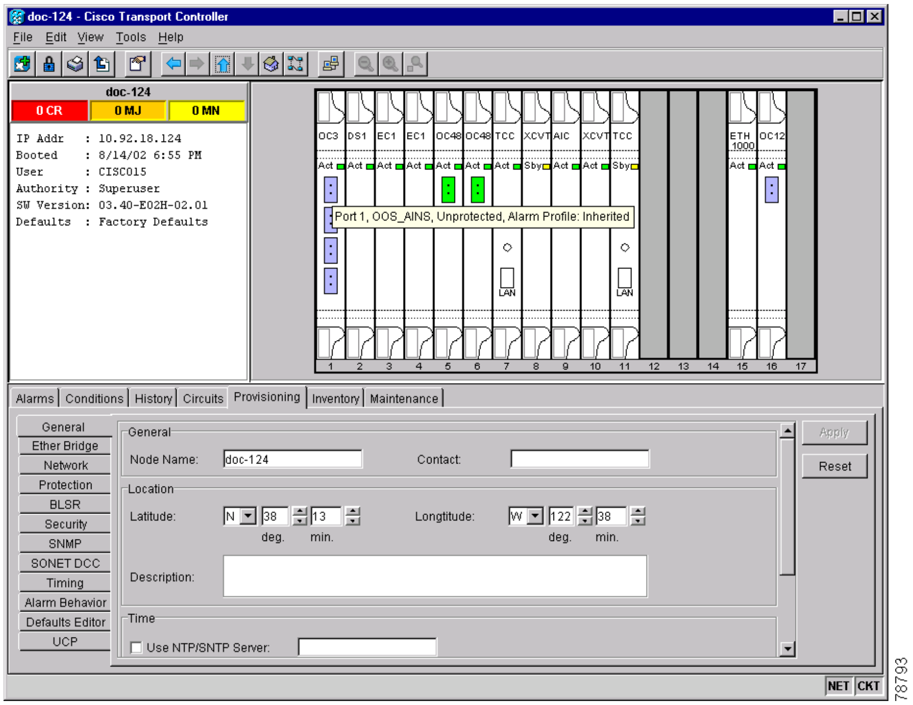
Table A-1 Change CTC Views

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 select **Open Node**. • From the CTC View menu, select **Go to Other Node**, then select 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.
Network view	• In node view, click the up arrow or the network view tool on the CTC toolbar. • From the View menu, select **Go To Network View**.
Card view	• In node view, double-click a card or right-click the card and select **Open Card**. • 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.

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 (Figure A-1).

Figure A-1 CTC node view showing popup information



doc-124 - Cisco Transport Controller

```
IP Addr   : 10.92.18.124
Booted    : 8/14/02 6:55 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Port 1, OOS_AINS, Unprotected, Alarm Profile: Inherited

Node Name: doc-124

Contact:

Latitude: N 38 deg. 13 min.

Longtitude: W 122 deg. 38 min.

Description:

☐ Use NTP/SNTP Server:

CTC Menu and Toolbar Options

The CTC window menu bar and toolbar provide primary CTC functions. Table A-2 shows the actions that are available from the CTC menu and toolbar.

Table A-2 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node		Adds a node to the current session. See the "DLP-62 Add a Node to the Current Session or Login Group" task on page 3-25.
	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-138 Print CTC Data" task on page 7-2.

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
	Export	⎘	Exports CTC data. See the "DLP-139 Export CTC Data" task on page 7-3.
	Exit	n/a	Closes the CTC session
Edit	Preferences	☑	Displays the Preferences dialog box: General tab—Allows you to customize the network view. See the "DLP-145 Change the Network View Background Color" task on page 10-9 and "DLP-147 Apply a Custom Network View Background Map" task on page 10-11. Also allows you to change the alarm history and events defaults. Login Node Group tab— Allows you to create login node groups. See the "DLP-61 Create Login Node Groups" task on page 3-24. Map—Allows you to change the network background image. Circuit—Allows you to change the color of circuit spans. See the "DLP-232 Change Active and Standby Span Color" task on page 9-9. Firewall—Sets the IIOP listener ports for access to the ONS 15454 through a firewall. See the "NTP-27 Set Up the ONS 15454 for Firewall Access" procedure on page 4-15.
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 and Go to Next is similar to a web browser forward/backward navigation.
	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	n/a	Displays a dialog box allowing you to enter a network node that you want to view. You can enter the node name or its IP address.
	Show Status Bar	n/a	Click this item to display/hide the status bar at the bottom of the CTC window
	Show Tool Bar	n/a	Click this item to display/hide the CTC toolbar.
n/a	n/a	🔍−	Zooms out the network view area (toolbar only)
n/a	n/a	🔍+	Zooms in network view area (toolbar only)

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
n/a	n/a	🔍	Zooms in a selected network view area (toolbar only)
Tools	Circuits	n/a	Displays the following options: • Repair Circuits—Repairs incomplete circuits following replacement of the ONS 15454 AIP board. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information. • Set Path Selector Attributes—Allows you to edit UPSR circuit path selector attributes. See the "DLP-233 Edit UPSR Circuit Path Selectors" task on page 9-10. • Set Circuit State—Allows you to change a circuit state. See the "DLP-230 Change a Circuit State" task on page 9-7. • Roll Circuit—*For future use*
	Manage VLANs	n/a	Displays a list of VLANs that have been created and allows you to delete or create new VLANs. See the Chapter 6, "NTP-130 Create a Unidirectional DS-1 Circuit with Multiple Drops.".
	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*.

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 right-clicking an item and selecting actions from shortcut menus. Table A-3 lists the CTC window mouse shortcuts.

Table A-3 CTC Window Mouse Shortcuts

Technique	Description
Double-Click	• A node in network view to display the node view • A card in node view to display the card view
Right-Click	• Network view graphic area—Displays a menu where you can create a new domain, change the position and zoom level of the graphic image, and change the background image and color. • Node in network view—Displays a menu where you can open the node, provision circuits, update circuits with a new node, and reset the node icon position to the longitude and latitude set on the Provisioning > General tab. • Span in network view—Displays a menu where you can view information about the source and destination ports, the span's protection scheme, and the span's optical or electrical level. You can also display the Circuits on Span dialog box, which displays additional span information and allows you to perform UPSR protection switching. • Card in node view—Displays a menu where you can open, delete, reset, and change cards. The card that is selected determines the commands that are displayed. • Empty slot in node view—Displays a menu with cards that you can select to pre-provision 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 • Over card in node view—Displays card type and card status • Over card port in node view—Displays port number and port status

Node View Shortcuts

Table A-4 shows actions on ONS 15454 cards that you can perform by moving your mouse over the CTC window.

Table A-4 Performing Node View Card Shortcuts

Action	Shortcut
Display card information	In node view, move your mouse over cards in the graphic to display tooltips with the card type, card status (active or standby), the highest level of alarm (if any), and the alarm profile used by the card. In card view, move your mouse over the card ports in the graphic to display tooltips with the port status (active or standby) and the alarm profile used by the port.
Open, reset, or delete a card	In node view, right-click a card. Select **Open** to display the card in card view, **Reset**, to reset the card, or **Delete** to delete it.
Pre-provision a slot	In node view, right-click an empty slot. Select 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 and select **Change Card**. On the Change Card dialog box, select 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-5 lists the actions that are available from the network view.

Table A-5 Performing 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, choose **Open Node** from the shortcut menu • Click a node and choose **Go to Selected Object View** from the CTC View menu • From the View menu, choose **Go To Other Node**. Select a node from the Select Node dialog box • Double-click a node alarm or event in the Alarms or History tabs
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 select the node where you want to provision the circuit. For circuit creation procedures, see Chapter 6, “Create Circuits and VT Tunnels.”

Table A-5 Performing 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. On the shortcut menu, select **Go To [node/slot/port]** for the drop port you want to view. CTC displays the card in card view.
Display span properties	Any of the following: • Move mouse over a span; properties near the span • Click a span; properties display in the upper left corner of the window • Right-click a span; properties display at the top of the shortcut menu
Perform a UPSR protection switch for an entire span	Right-click a network span and click **Circuits**. On the Circuits on Span dialog box, switch options are displayed in the UPSR Span Switching field.
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 12, "Upgrade Cards and Spans."

Table Display Options

Right-clicking a table column displays a menuTable A-6 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

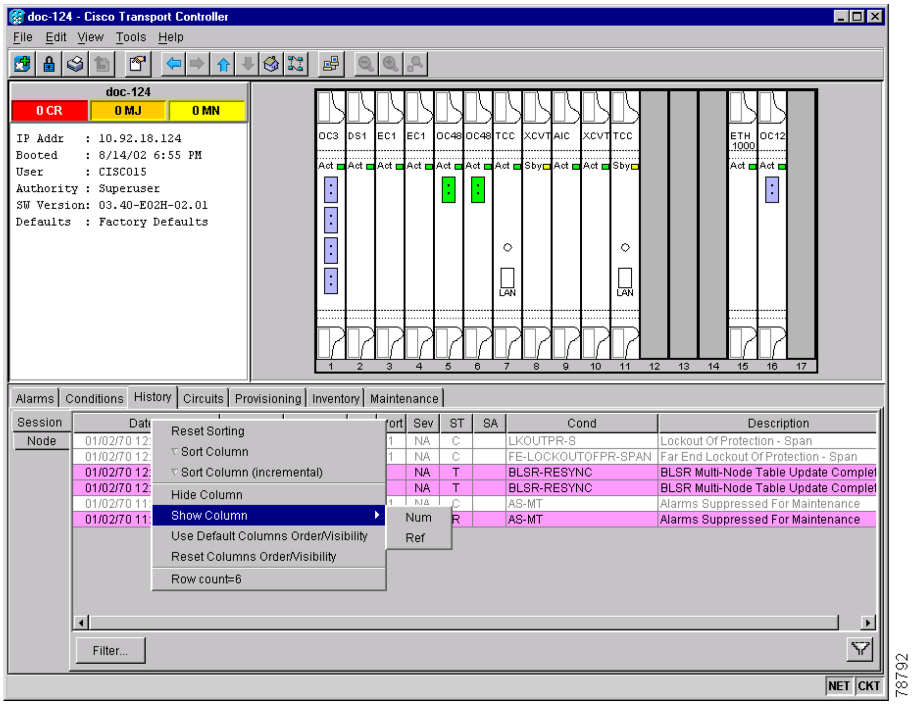
Table A-6 Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Left click while dragging the header separator to the right or left	N/A
Rearrange column order	Left click while dragging the column header to the right or left	N/A
Reset column order	N/A	Choose Reset Columns Order/Visibility
Hide column	N/A	Choose Hide Column
Display a hidden column	N/A	Choose Show Column>[column name]
Display all hidden columns	N/A	Choose Reset Columns Order/Visibility
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending)	Choose Sort Column
Sort table (secondary sorting keys)	Press the Shift key and simultaneously click the column header	Choose Sort Column (incremental)

Table A-6 Table Display Options (continued)

Task	Click	Right-Click Shortcut Menu
Reset sorting	N/A	Choose Reset Sorting
View table row count	N/A	View Row count; it is the last item on the shortcut menu

Figure A-2 The right-click table shortcut menu that customizes table appearance


doc-124 - Cisco Transport Controller
File Edit View Tools Help
doc-124
0 CR
0 MJ
0 MN
OC3 DS1 EC1 EC1 OC48 OC48 TCC XCVT AIC XCVT TCC ETH 1000 OC12
Act Act Act Act Act Act Act Sby Act Act Sby Act Act
LAN
LAN
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Session
Node
Reset Sorting
Sort Column
Sort Column (incremental)
Hide Column
Show Column
Use Default Columns Order/Visibility
Reset Columns Order/Visibility
Row count=6
Num
Ref
Filter...
NET CKT
78792

```
IP Addr    : 10.92.18.124
Booted     : 8/14/02 6:55 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.40-E02H-02.01
Defaults   : Factory Defaults
```

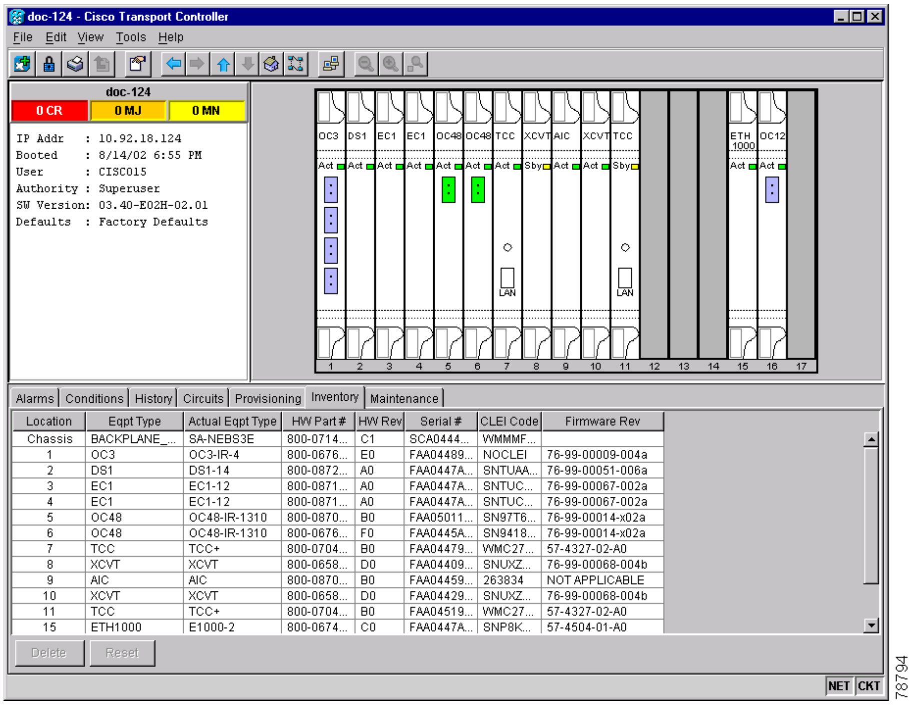
Date	ort	Sev	ST	SA	Cond	Description
01/02/70 12:	1	NA	C		LKOUTPR-S	Lockout Of Protection - Span
01/02/70 12:	1	NA	C		FE-LOCKOUTOFPR-SPAN	Far End Lockout Of Protection - Span
01/02/70 12:		NA	T		BLSR-RESYNC	BLSR Multi-Node Table Update Complet
01/02/70 12:		NA	T		BLSR-RESYNC	BLSR Multi-Node Table Update Complet
01/02/70 11:	1	NA	C		AS-MT	Alarms Suppressed For Maintenance
01/02/70 11:			R		AS-MT	Alarms Suppressed For Maintenance

Equipment Inventory

In node view, the Inventory tab (Figure A-3) displays information about the ONS 15454 equipment, including:

- *Location*—Where the equipment is installed, either chassis or slot number
- *Eqpt Type*—The equipment type, for example, OC-12 or DS-1.
- *Actual Eqpt Type*—The actual equipment type, for example, OC48-IR-1
- *HW Part #*—Hardware part number; this number is printed on the top of the card or equipment piece.
- *HW Rev*—Hardware revision number
- *Serial #*—Equipment serial number; this number is unique to each card
- *CLEI Code*—Common Language Equipment Identifier code
- *Firmware Rev*—Revision number of the software used by the ASIC chip installed on the ONS 15454 cards

Figure A-3 Displaying ONS 15454 hardware information



```
IP Addr   : 10.92.18.124
Booted    : 8/14/02 6:55 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Location	Eqpt Type	Actual Eqpt Type	HW Part #	HW Rev	Serial #	CLEI Code	Firmware Rev
Chassis	BACKPLANE_...	SA-NEBS3E	800-0714...	C1	SCA0444...	WMMMF...	
1	OC3	OC3-IR-4	800-0676...	E0	FAA04489...	NOCLEI	76-99-00009-004a
2	DS1	DS1-14	800-0872...	A0	FAA0447A...	SNTUAA...	76-99-00051-006a
3	EC1	EC1-12	800-0871...	A0	FAA0447A...	SNTUC...	76-99-00067-002a
4	EC1	EC1-12	800-0871...	A0	FAA0447A...	SNTUC...	76-99-00067-002a
5	OC48	OC48-IR-1310	800-0870...	B0	FAA05011...	SN97T6...	76-99-00014-x02a
6	OC48	OC48-IR-1310	800-0676...	F0	FAA0445A...	SN9418...	76-99-00014-x02a
7	TCC	TCC+	800-0704...	B0	FAA04479...	WMC27...	57-4327-02-A0
8	XCVT	XCVT	800-0658...	D0	FAA04409...	SNUXZ...	76-99-00068-004b
9	AIC	AIC	800-0870...	B0	FAA04459...	263834	NOT APPLICABLE
10	XCVT	XCVT	800-0658...	D0	FAA04429...	SNUXZ...	76-99-00068-004b
11	TCC	TCC+	800-0704...	B0	FAA04519...	WMC27...	57-4327-02-A0
15	ETH1000	E1000-2	800-0674...	C0	FAA0447A...	SNP8K...	57-4504-01-A0

APPENDIX B

Shelf Assembly Specifications

This appendix contains hardware and software specifications for the ONS 15454.

Bandwidth

- Total bandwidth: 240 Gbps
- Data plane bandwidth: 160 Gbps
- SONET plane bandwidth: 80 Gbps

Slot Assignments

- Total card slots: 17
- Multispeed slots (any traffic card except OC48 IR 1310, OC48 LR/ELR 1550, and OC192 LR 1550 cards): Slots 1–4, 14–17
- High-speed slots (any traffic card including OC48 IR 1310, OC48 LR/ELR 1550, and OC192 LR 1550 cards): Slots 5, 6, 12, 13
- TCC+ (Timing Communication and Control): Slots 7, 11
- XC/XCVT/XC10G (Cross Connect): Slots 8, 10
- AIC (Alarm Interface Card), AIC-I: Slot 9

Cards

- TCC+
- XC
- XCVT
- XC10G
- AIC
- AIC-I
- EC1-12

- DS1-14
- DS1N-14
- DS3-12
- DS3N-12
- DS3-12E
- DS3N-12E
- DS3XM-6
- OC3 IR 4 1310
- OC12 IR 1310
- OC12 LR 1310
- OC12 LR 1550
- Quad OC12
- OC48 IR 1310
- OC48 LR 1550
- OC48 IR/STM16 SH AS 1310
- OC48 LR/STM16 LH AS 1550
- OC192 LR 1550
- OC48 ELR 200 Ghz ITU
- OC48 ELR 100 Ghz ITU
- E100T-12
- E1000-2
- E100T-G
- E1000-2-G
- G1000-4

Note The OC-3, OC-12, OC-48, and E1000-2 cards are Class 1 laser products (IEC 60825-1 2001-01/Class I laser product (21CFR 1040.10 and 1040.11).

Note The OC-192 card is a Class 1M laser product ((IEC 60825-1 2001-01)/Class I laser product (21CFR 1040.10 and 1040.11).

Configurations

- Two-fiber UPSR
- Path protected mesh network (PPMN)
- Two-fiber BLSR
- Four-fiber BLSR

- Add-drop multiplexer
- Terminal mode
- Regenerator mode

Cisco Transport Controller

- 10 Base-T
- TCC+ access: RJ-45 connector
- Backplane access: LAN pin field

External LAN Interface

- 10 Base-T Ethernet
- Backplane access: LAN pin field

TL1 Craft Interface

- Speed: 9600 bps
- TCC+ access: RS-232 DB-9 type connector
- Backplane access: CRAFT pin field

Modem Interface

- Hardware flow control
- TCC+: RS-232 DB-9 type connector

Alarm Interface

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: 0.045mm, -48V, 50 mA
- Backplane access: Alarm pin fields

EIA Interface

- 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

Nonvolatile Memory

64 MB, 3.0V FLASH memory

BITS Interface

- 2 DS-1 BITS inputs
- 2 derived DS-1 outputs
- Backplane access: BITS pin field

System Timing

- 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

- Input power: -48 VDC
- Power consumption: 55W (fan tray only); 650W (maximum draw w/cards)
- Power requirements: -42 to -57 VDC
- Power terminals: #6 Lug
- ANSI shelf: 100 Amp fuse panel (minimum 30 Amp fuse per shelf)
  NEBS3 shelf: 80 Amp fuse panel (minimum 20 Amp fuse per shelf

Environmental Specifications

- Operating Temperature: 0 to +55 degrees Celsius; -40 to +65 degrees Celsius with industrial temperature rated cards
- Operating Humidity: 5 - 95%, non-condensing

Dimensions

- Height: 18.5 inches (40.7 cm)
- Width: 19 or 23 inches (41.8 or 50.6 cm) with mounting ears attached
- Depth: 12 inches (26.4 cm) (5 inch projection from rack)
- Weight: 55 lbs. (empty)

APPENDIX C

Network Element Defaults

This appendix describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15454. It includes descriptions of card default settings and node default settings and provides procedures for importing, exporting and editing the settings. Ethernet card settings are not included in the factory-configured settings.

To change card settings individually (that is, without changing the defaults), see Chapter 11, "Change Card Settings." To change node settings without changing the defaults, see Chapter 10, "Change Node Settings."

Network Element Defaults Description

The NE defaults are pre-installed on each ONS 15454 (on the TCC+ cards). They also ship as a file called 15454-defaults on the CTC software CD in the event you want to import the defaults onto existing TCC+ cards. The NE defaults include card-level and node-level defaults.

Changes made manually using Chapter 11, "Change Card Settings"override default settings. If you use the Defaults Editor or import a new defaults file, that is, if defaults are changed, the changes apply only to cards installed subsequently (after the defaults change) or to slots pre-provisioned subsequently. A new defaults file will not take effect for cards already installed when the change takes place or for slots already pre-provisioned when the change takes place.

Changes made manually to the node-level default settings (either when you initially turn up a node or change node settings later) override the default settings. If you change the default settings, using either the Defaults Editor or by importing a new defaults file, the new defaults take effect immediately for all settings except those relating to UPSR, BLSR, or 1+1 protection.

Use the following procedures if you need to edit, import, or export NE defaults.

NTP-164 Edit Network Element Defaults

Purpose	This procedure edits the NE defaults using the NE Defaults Editor. The new defaults can either be applied only to the node on which they are edited or exported to a file and imported for use on other nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 After logging into the node, click the **Provisioning > Defaults Editor** tabs.

Step 2 Under Defaults Selector, choose either a card (if editing card-level defaults) or NODE (if editing node-level defaults). Clicking on the node name (at the top of the Defaults Selector column) lists all available NE defaults (both node- and card-level) under Property Name.

Step 3 Locate a default you want to change under Property Name.

Step 4 Click in the **Default Value** column for the default property you are changing and either choose a value from the drop-down menu (available for some node-level settings only), or type in the desired new value.

Note Clicking **Reset** before clicking **Apply** will return all values to their original setting.

Step 5 Click **Apply** (click in the **Property Name** column to activate the Apply button if it is unavailable). You can modify multiple default values before applying the changes.

Step 6 If you are modifying node-level defaults, a dialog box opens telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

Note Changes to node settings take effect upon clicking **Apply**. Changes to the IIOP Listener Port setting reboots the TCC+. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed or slots that are pre-provisioned for cards. Card settings must be manually changed by opening the cards (or pre-provisioned card slot). For procedures to change card settings, see Chapter 11, “Change Card Settings.”

NTP-165 Import Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults Editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 After logging into the node, click the **Provisioning > Defaults Editor** tabs.

Step 2 Click **Import**.

Step 3 Click **Browse** and browse to the file you are importing if the correct file name and location of the desired file do not appear in the Import Defaults from File dialog box.

Step 4 When the correct file name and location appear in the dialog box (the correct file name is 15454-defaults if you are importing the factory defaults), click **OK**.

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 5 Click **Apply**.

Step 6 If you are modifying node-level defaults, a dialog box opens telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

Note Changes to node settings take effect upon clicking **Apply**. Changes to the IIOP Listener Port setting reboots the TCC+. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed or slots that are pre-provisioned for cards. Card settings must be manually changed by opening the cards (or the pre-provisioned card slots). For procedures to change card settings, see Chapter 11, “Change Card Settings.”

NTP-166 Export Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults Editor. The exported defaults can be imported to other nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-60 Log into CTC, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 After logging into the node, click the **Provisioning > Defaults Editor** tabs.

Step 2 Click **Export**.

Step 3 Click **Browse** and browse to the location where you want to export the file if it does not appear in the Export Defaults to File dialog box.

Step 4 Change the file name to something easy to remember (the file name has no extension).

Step 5 Click **OK**.

Card Default Settings

The tables in this section list the default settings for each card. Cisco provides the following settings pre-provisioned for the ONS 15454 optical and electrical cards:

- Soak Time (all cards) is the length of time that elapses between an AINS port receiving a valid signal and when it automatically changes to in-service status.
- Line Coding (DS-1 Cards) defines the DS-1 transmission coding type that is used.
- Line Length (DS-1, DS-3, and EC-1 Cards) defines the distance (in feet) from the backplane connection to the next termination point.
- Line Type (DS-1, DS3E, and DS3XM-6 cards) defines the type of framing used.
- Port State (all cards) sets the port to one of the four available states (IS, OOS, OOS_MT, or OOS_AINS), depending on whether you need ports in or out of service. See the "DLP-214 Change the Service State for a Port" task on page 5-5 for a complete description of the port states.
- SF BER Level (OC-N Cards) defines the signal fail bit error rate.
- SD BER Level (OC-N Cards) defines the signal degrade bit error rate.
- Enable Synch Messages (OC-N Cards) enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.
- PJ Sts Mon (EC-1 card and OC-N Cards) sets the STS that will be used for pointer justification. If set to 0, no STS is monitored.
- Rx Equalization (EC-1 Card) can be turned off if the line length is short or the environment is extremely cold.
- STS IPPM Enabled (OC-N cards) enables intermediate-path performance monitoring on a node for transparent monitoring of a channel that does not terminate on that node.

- Send Do Not Use (OC-N cards) sends a DUS message on the S1 byte when enabled.
- Far End Inhibit Loopback (DS3E and DS3XM-6 cards) enables DS3E or DS3XM-6 cards to inhibit loopbacks on the far end.
- PM Threshold Settings (all cards) set the performance monitoring parameters for gathering performance data and detecting problems early. For definitions of the performance monitoring parameters, refer to the *Cisco ONS 15454 Reference Manual*.

Table C-1 lists the DS-1 Card default settings.

Table C-1 DS-1 Card Default Settings

Property Name	Default Value
DS1.config.AINSSoakTime	08:00 (hours:mins)
DS1.config.LineCoding	AMI
DS1.config.LineLength	0-131 (feet)
DS1.config.LineType	D4
DS1.config.State	OOS
DS1.pmthresholds.line.nearend.15min.CV	13340 (BPV count)
DS1.pmthresholds.line.nearend.15min.ES	65 (seconds)
DS1.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
DS1.pmthresholds.line.nearend.15min.SES	10 (seconds)
DS1.pmthresholds.line.nearend.1day.CV	133400 (BPV count)
DS1.pmthresholds.line.nearend.1day.ES	648 (seconds)
DS1.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
DS1.pmthresholds.line.nearend.1day.SES	100 (seconds)
DS1.pmthresholds.path.nearend.15min.AISS	10 (seconds)
DS1.pmthresholds.path.nearend.15min.CV	13296 (BIP count)
DS1.pmthresholds.path.nearend.15min.ES	65 (seconds)
DS1.pmthresholds.path.nearend.15min.SAS	2 (seconds)
DS1.pmthresholds.path.nearend.15min.SES	10 (seconds)
DS1.pmthresholds.path.nearend.15min.UAS	10 (seconds)
DS1.pmthresholds.path.nearend.1day.AISS	10 (seconds)
DS1.pmthresholds.path.nearend.1day.CV	132960 (BIP count)
DS1.pmthresholds.path.nearend.1day.ES	648 (seconds)
DS1.pmthresholds.path.nearend.1day.SAS	17 (seconds)
DS1.pmthresholds.path.nearend.1day.SES	100 (seconds)
DS1.pmthresholds.path.nearend.1day.UAS	10 (seconds)
DS1.pmthresholds.sts.farend.15min.CV	15 (B3 count)
DS1.pmthresholds.sts.farend.15min.ES	12 (seconds)
DS1.pmthresholds.sts.farend.15min.FC	10 (count)
DS1.pmthresholds.sts.farend.15min.SES	3 (seconds)
DS1.pmthresholds.sts.farend.15min.UAS	10 (seconds)
DS1.pmthresholds.sts.farend.1day.CV	125 (B3 count)
DS1.pmthresholds.sts.farend.1day.ES	100 (seconds)
DS1.pmthresholds.sts.farend.1day.FC	10 (count)
DS1.pmthresholds.sts.farend.1day.SES	7 (seconds)
DS1.pmthresholds.sts.farend.1day.UAS	10 (seconds)
DS1.pmthresholds.sts.nearend.15min.CV	15 (B3 count)

Table C-1 DS-1 Card Default Settings (continued)

Property Name	Default Value
DS1.pmthresholds.sts.nearend.15min.ES	12 (seconds)
DS1.pmthresholds.sts.nearend.15min.FC	10 (count)
DS1.pmthresholds.sts.nearend.15min.SES	3 (seconds)
DS1.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
DS1.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
DS1.pmthresholds.sts.nearend.1day.ES	100 (seconds)
DS1.pmthresholds.sts.nearend.1day.FC	10 (count)
DS1.pmthresholds.sts.nearend.1day.SES	7 (seconds)
DS1.pmthresholds.sts.nearend.1day.UAS	10 (seconds)
DS1.pmthresholds.vt.farend.15min.CV	15 (BIP8 count)
DS1.pmthresholds.vt.farend.15min.ES	12 (seconds)
DS1.pmthresholds.vt.farend.15min.SES	3 (seconds)
DS1.pmthresholds.vt.farend.15min.UAS	10 (seconds)
DS1.pmthresholds.vt.farend.1day.CV	125 (BIP8 count)
DS1.pmthresholds.vt.farend.1day.ES	100 (seconds)
DS1.pmthresholds.vt.farend.1day.SES	7 (seconds)
DS1.pmthresholds.vt.farend.1day.UAS	10 (seconds)
DS1.pmthresholds.vt.nearend.15min.CV	15 (BIP8 count)
DS1.pmthresholds.vt.nearend.15min.ES	12 (seconds)
DS1.pmthresholds.vt.nearend.15min.SES	3 (seconds)
DS1.pmthresholds.vt.nearend.15min.UAS	10 (seconds)
DS1.pmthresholds.vt.nearend.1day.CV	125 (BIP8 count)
DS1.pmthresholds.vt.nearend.1day.ES	100 (seconds)
DS1.pmthresholds.vt.nearend.1day.SES	7 (seconds)
DS1.pmthresholds.vt.nearend.1day.UAS	10 (seconds)

Table C-2 Lists the DS-3 Card default settings.

Table C-2 DS-3 Card Default Settings

Property Name	Default Value
DS3.config.AINSSoakTime	08:00 (hours:mins)
DS3.config.LineLength	0-225 (feet)
DS3.config.State	OOS
DS3.pmthresholds.line.nearend.15min.CV	387 (BPV count)
DS3.pmthresholds.line.nearend.15min.ES	25 (seconds)
DS3.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
DS3.pmthresholds.line.nearend.15min.SES	4 (seconds)

Table C-2 DS-3 Card Default Settings (continued)

Property Name	Default Value
DS3.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
DS3.pmthresholds.line.nearend.1day.ES	250 (seconds)
DS3.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
DS3.pmthresholds.line.nearend.1day.SES	40 (seconds)
DS3.pmthresholds.sts.farend.15min.CV	15 (G1 count)
DS3.pmthresholds.sts.farend.15min.ES	12 (seconds)
DS3.pmthresholds.sts.farend.15min.FC	10 (count)
DS3.pmthresholds.sts.farend.15min.SES	3 (seconds)
DS3.pmthresholds.sts.farend.15min.UAS	10 (seconds)
DS3.pmthresholds.sts.farend.1day.CV	125 (G1 count)
DS3.pmthresholds.sts.farend.1day.ES	100 (seconds)
DS3.pmthresholds.sts.farend.1day.FC	10 (count)
DS3.pmthresholds.sts.farend.1day.SES	7 (seconds)
DS3.pmthresholds.sts.farend.1day.UAS	10 (seconds)
DS3.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
DS3.pmthresholds.sts.nearend.15min.ES	12 (seconds)
DS3.pmthresholds.sts.nearend.15min.FC	10 (count)
DS3.pmthresholds.sts.nearend.15min.SES	3 (seconds)
DS3.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
DS3.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
DS3.pmthresholds.sts.nearend.1day.ES	100 (seconds)
DS3.pmthresholds.sts.nearend.1day.FC	10 (count)
DS3.pmthresholds.sts.nearend.1day.SES	7 (seconds)
DS3.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-3 lists the DS3E Card default settings.

Table C-3 DS3E Card Default Settings

Property Name	Default Value
DS3E.config.AINSSoakTime	08:00 (hours:mins)
DS3E.config.FeInhibitLpbk	FALSE
DS3E.config.LineLength	0-225 (feet)
DS3E.config.LineType	UNFRAMED
DS3E.config.State	OOS
DS3E.pmthresholds.cpbitpath.farend.15min.AISS	10 (seconds)
DS3E.pmthresholds.cpbitpath.farend.15min.CV	382 (BIP count)
DS3E.pmthresholds.cpbitpath.farend.15min.ES	25 (seconds)

Table C-3 DS3E Card Default Settings (continued)

Property Name	Default Value
DS3E.pmthresholds.cpbitpath.farend.15min.SAS	2 (seconds)
DS3E.pmthresholds.cpbitpath.farend.15min.SES	4 (seconds)
DS3E.pmthresholds.cpbitpath.farend.15min.UAS	10 (seconds)
DS3E.pmthresholds.cpbitpath.farend.1day.AISS	10 (seconds)
DS3E.pmthresholds.cpbitpath.farend.1day.CV	3820 (BIP count)
DS3E.pmthresholds.cpbitpath.farend.1day.ES	250 (seconds)
DS3E.pmthresholds.cpbitpath.farend.1day.SAS	8 (seconds)
DS3E.pmthresholds.cpbitpath.farend.1day.SES	40 (seconds)
DS3E.pmthresholds.cpbitpath.farend.1day.UAS	10 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.15min.AISS	10 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.15min.CV	382 (BIP count)
DS3E.pmthresholds.cpbitpath.nearend.15min.ES	25 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.15min.SAS	2 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.15min.SES	4 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.15min.UAS	10 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.1day.AISS	10 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.1day.CV	3820 (BIP count)
DS3E.pmthresholds.cpbitpath.nearend.1day.ES	250 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.1day.SAS	8 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.1day.SES	40 (seconds)
DS3E.pmthresholds.cpbitpath.nearend.1day.UAS	10 (seconds)
DS3E.pmthresholds.line.nearend.15min.CV	387 (BPV count)
DS3E.pmthresholds.line.nearend.15min.ES	25 (seconds)
DS3E.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
DS3E.pmthresholds.line.nearend.15min.SES	4 (seconds)
DS3E.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
DS3E.pmthresholds.line.nearend.1day.ES	250 (seconds)
DS3E.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
DS3E.pmthresholds.line.nearend.1day.SES	40 (seconds)
DS3E.pmthresholds.pbitpath.nearend.15min.AISS	10 (seconds)
DS3E.pmthresholds.pbitpath.nearend.15min.CV	382 (BIP count)
DS3E.pmthresholds.pbitpath.nearend.15min.ES	25 (seconds)
DS3E.pmthresholds.pbitpath.nearend.15min.SAS	2 (seconds)
DS3E.pmthresholds.pbitpath.nearend.15min.SES	4 (seconds)
DS3E.pmthresholds.pbitpath.nearend.15min.UAS	10 (seconds)
DS3E.pmthresholds.pbitpath.nearend.1day.AISS	10 (seconds)

Table C-3 DS3E Card Default Settings (continued)

Property Name	Default Value
DS3E.pmthresholds.pbitpath.nearend.1day.CV	3820 (BIP count)
DS3E.pmthresholds.pbitpath.nearend.1day.ES	250 (seconds)
DS3E.pmthresholds.pbitpath.nearend.1day.SAS	8 (seconds)
DS3E.pmthresholds.pbitpath.nearend.1day.SES	40 (seconds)
DS3E.pmthresholds.pbitpath.nearend.1day.UAS	10 (seconds)
DS3E.pmthresholds.sts.farend.15min.CV	15 (G1 count)
DS3E.pmthresholds.sts.farend.15min.ES	12 (seconds)
DS3E.pmthresholds.sts.farend.15min.FC	10 (count)
DS3E.pmthresholds.sts.farend.15min.SES	3 (seconds)
DS3E.pmthresholds.sts.farend.15min.UAS	10 (seconds)
DS3E.pmthresholds.sts.farend.1day.CV	125 (G1 count)
DS3E.pmthresholds.sts.farend.1day.ES	100 (seconds)
DS3E.pmthresholds.sts.farend.1day.FC	10 (count)
DS3E.pmthresholds.sts.farend.1day.SES	7 (seconds)
DS3E.pmthresholds.sts.farend.1day.UAS	10 (seconds)
DS3E.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
DS3E.pmthresholds.sts.nearend.15min.ES	12 (seconds)
DS3E.pmthresholds.sts.nearend.15min.FC	10 (count)
DS3E.pmthresholds.sts.nearend.15min.SES	3 (seconds)
DS3E.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
DS3E.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
DS3E.pmthresholds.sts.nearend.1day.ES	100 (seconds)
DS3E.pmthresholds.sts.nearend.1day.FC	10 (count)
DS3E.pmthresholds.sts.nearend.1day.SES	7 (seconds)
DS3E.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-4 lists the DS3XM-6 Card default settings.

Table C-4 DS3XM-6 Card Default Settings

Property Name	Default Value
DS3XM.config.AINSSoakTime	08:00 (hours:mins)
DS3XM.config.FeInhibitLpbk	FALSE
DS3XM.config.LineLength	0-225 (feet)
DS3XM.config.LineType	M23
DS3XM.config.State	OOS
DS3XM.pmthresholds.cpbitpath.farend.15min.AISS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.15min.CV	382 (BIP count)

Table C-4 DS3XM-6 Card Default Settings (continued)

Property Name	Default Value
DS3XM.pmthresholds.cpbitpath.farend.15min.ES	25 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.15min.SAS	2 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.15min.SES	4 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.1day.AISS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.1day.CV	3820 (BIP count)
DS3XM.pmthresholds.cpbitpath.farend.1day.ES	250 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.1day.SAS	8 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.1day.SES	40 (seconds)
DS3XM.pmthresholds.cpbitpath.farend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.15min.AISS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.15min.CV	382 (BIP count)
DS3XM.pmthresholds.cpbitpath.nearend.15min.ES	25 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.15min.SAS	2 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.15min.SES	4 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.1day.AISS	10 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.1day.CV	3820 (BIP count)
DS3XM.pmthresholds.cpbitpath.nearend.1day.ES	250 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.1day.SAS	8 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.1day.SES	40 (seconds)
DS3XM.pmthresholds.cpbitpath.nearend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.ds1path.nearend.15min.AISS	63 (seconds)
DS3XM.pmthresholds.ds1path.nearend.15min.ES	7 (seconds)
DS3XM.pmthresholds.ds1path.nearend.15min.SAS	63 (seconds)
DS3XM.pmthresholds.ds1path.nearend.15min.SES	3 (seconds)
DS3XM.pmthresholds.ds1path.nearend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.ds1path.nearend.1day.AISS	10 (seconds)
DS3XM.pmthresholds.ds1path.nearend.1day.ES	648 (seconds)
DS3XM.pmthresholds.ds1path.nearend.1day.SAS	17 (seconds)
DS3XM.pmthresholds.ds1path.nearend.1day.SES	100 (seconds)
DS3XM.pmthresholds.ds1path.nearend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.line.nearend.15min.CV	387 (BPV count)
DS3XM.pmthresholds.line.nearend.15min.ES	25 (seconds)
DS3XM.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
DS3XM.pmthresholds.line.nearend.15min.SES	4 (seconds)

Table C-4 DS3XM-6 Card Default Settings (continued)

Property Name	Default Value
DS3XM.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
DS3XM.pmthresholds.line.nearend.1day.ES	250 (seconds)
DS3XM.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
DS3XM.pmthresholds.line.nearend.1day.SES	40 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.15min.AISS	10 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.15min.CV	382 (BIP count)
DS3XM.pmthresholds.pbitpath.nearend.15min.ES	25 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.15min.SAS	2 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.15min.SES	4 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.1day.AISS	10 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.1day.CV	3820 (BIP count)
DS3XM.pmthresholds.pbitpath.nearend.1day.ES	250 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.1day.SAS	8 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.1day.SES	40 (seconds)
DS3XM.pmthresholds.pbitpath.nearend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.sts.farend.15min.CV	15 (B3 count)
DS3XM.pmthresholds.sts.farend.15min.ES	12 (seconds)
DS3XM.pmthresholds.sts.farend.15min.FC	10 (count)
DS3XM.pmthresholds.sts.farend.15min.SES	3 (seconds)
DS3XM.pmthresholds.sts.farend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.sts.farend.1day.CV	125 (B3 count)
DS3XM.pmthresholds.sts.farend.1day.ES	100 (seconds)
DS3XM.pmthresholds.sts.farend.1day.FC	10 (count)
DS3XM.pmthresholds.sts.farend.1day.SES	7 (seconds)
DS3XM.pmthresholds.sts.farend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
DS3XM.pmthresholds.sts.nearend.15min.ES	12 (seconds)
DS3XM.pmthresholds.sts.nearend.15min.FC	10 (count)
DS3XM.pmthresholds.sts.nearend.15min.SES	3 (seconds)
DS3XM.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
DS3XM.pmthresholds.sts.nearend.1day.ES	100 (seconds)
DS3XM.pmthresholds.sts.nearend.1day.FC	10 (count)
DS3XM.pmthresholds.sts.nearend.1day.SES	7 (seconds)
DS3XM.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-4 DS3XM-6 Card Default Settings (continued)

Property Name	Default Value
DS3XM.pmthresholds.vt.farend.15min.CV	15 (BIP8 count)
DS3XM.pmthresholds.vt.farend.15min.ES	12 (seconds)
DS3XM.pmthresholds.vt.farend.15min.SES	3 (seconds)
DS3XM.pmthresholds.vt.farend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.vt.farend.1day.CV	125 (BIP8 count)
DS3XM.pmthresholds.vt.farend.1day.ES	100 (seconds)
DS3XM.pmthresholds.vt.farend.1day.SES	7 (seconds)
DS3XM.pmthresholds.vt.farend.1day.UAS	10 (seconds)
DS3XM.pmthresholds.vt.nearend.15min.CV	15 (BIP8 count)
DS3XM.pmthresholds.vt.nearend.15min.ES	12 (seconds)
DS3XM.pmthresholds.vt.nearend.15min.SES	3 (seconds)
DS3XM.pmthresholds.vt.nearend.15min.UAS	10 (seconds)
DS3XM.pmthresholds.vt.nearend.1day.CV	125 (BIP8 count)
DS3XM.pmthresholds.vt.nearend.1day.ES	100 (seconds)
DS3XM.pmthresholds.vt.nearend.1day.SES	7 (seconds)
DS3XM.pmthresholds.vt.nearend.1day.UAS	10 (seconds)

Table C-5 lists the EC-1 Card default settings.

Table C-5 EC-1 Card Default Settings

Property Name	Default Value
EC1.config.line.AINSSoakTime	08:00 (hours:mins)
EC1.config.line.LineLength	0-255 (feet)
EC1.config.line.PJStsMon#	0 (STS #)
EC1.config.line.State	OOS
EC1.config.sts.IPPMEnabled	FALSE
EC1.pmthresholds.line.farend.15min.CV	1312 (B2 count)
EC1.pmthresholds.line.farend.15min.ES	87 (seconds)
EC1.pmthresholds.line.farend.15min.FC	10 (count)
EC1.pmthresholds.line.farend.15min.SES	1 (seconds)
EC1.pmthresholds.line.farend.15min.UAS	363 (seconds)
EC1.pmthresholds.line.farend.1day.CV	13120 (B2 count)
EC1.pmthresholds.line.farend.1day.ES	864 (seconds)
EC1.pmthresholds.line.farend.1day.FC	40 (count)
EC1.pmthresholds.line.farend.1day.SES	4 (seconds)
EC1.pmthresholds.line.farend.1day.UAS	10 (seconds)
EC1.pmthresholds.line.nearend.15min.CV	1312 (B2 count)

Table C-5 EC-1 Card Default Settings (continued)

Property Name	Default Value
EC1.pmthresholds.line.nearend.15min.ES	87 (seconds)
EC1.pmthresholds.line.nearend.15min.FC	10 (count)
EC1.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
EC1.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
EC1.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
EC1.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
EC1.pmthresholds.line.nearend.15min.PSC	1 (count)
EC1.pmthresholds.line.nearend.15min.PSD	300 (seconds)
EC1.pmthresholds.line.nearend.15min.SES	1 (seconds)
EC1.pmthresholds.line.nearend.15min.UAS	3 (seconds)
EC1.pmthresholds.line.nearend.1day.CV	1312 (B2 count)
EC1.pmthresholds.line.nearend.1day.ES	864 (seconds)
EC1.pmthresholds.line.nearend.1day.FC	40 (count)
EC1.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
EC1.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
EC1.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
EC1.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
EC1.pmthresholds.line.nearend.1day.PSC	5 (count)
EC1.pmthresholds.line.nearend.1day.PSD	600 (seconds)
EC1.pmthresholds.line.nearend.1day.SES	4 (seconds)
EC1.pmthresholds.line.nearend.1day.UAS	10 (seconds)
EC1.pmthresholds.section.nearend.15min.CV	10000 (B1 count)
EC1.pmthresholds.section.nearend.15min.ES	500 (seconds)
EC1.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
EC1.pmthresholds.section.nearend.15min.SES	500 (seconds)
EC1.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
EC1.pmthresholds.section.nearend.1day.ES	5000 (seconds)
EC1.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
EC1.pmthresholds.section.nearend.1day.SES	5000 (seconds)
EC1.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
EC1.pmthresholds.sts.nearend.15min.ES	12 (seconds)
EC1.pmthresholds.sts.nearend.15min.FC	10 (count)
EC1.pmthresholds.sts.nearend.15min.SES	3 (seconds)
EC1.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
EC1.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
EC1.pmthresholds.sts.nearend.1day.ES	100 (seconds)

Table C-5 EC-1 Card Default Settings (continued)

Property Name	Default Value
EC1.pmthresholds.sts.nearend.1day.FC	10 (count)
EC1.pmthresholds.sts.nearend.1day.SES	7 (seconds)
EC1.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-6 lists the OC-3 cards' default settings.

Table C-6 OC-3 Card Default Settings

Property Name	Default Value
OC3.config.line.AINSSoakTime	08:00 (hours:mins)
OC3.config.line.EnableSyncMsg	TRUE
OC3.config.line.PJStsMon#	0 (STS #)
OC3.config.line.SDBER	1E-7
OC3.config.line.SFBER	1E-4
OC3.config.line.SendDoNotUse	FALSE
OC3.config.line.State	OOS
OC3.config.sts.IPPMEnabled	FALSE
OC3.pmthresholds.line.farend.15min.CV	1312 (B2 count)
OC3.pmthresholds.line.farend.15min.ES	87 (seconds)
OC3.pmthresholds.line.farend.15min.FC	10 (count)
OC3.pmthresholds.line.farend.15min.SES	1 (seconds)
OC3.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC3.pmthresholds.line.farend.1day.CV	13120 (B2 count)
OC3.pmthresholds.line.farend.1day.ES	864 (seconds)
OC3.pmthresholds.line.farend.1day.FC	40 (count)
OC3.pmthresholds.line.farend.1day.SES	4 (seconds)
OC3.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC3.pmthresholds.line.nearend.15min.CV	1312 (B2 count)
OC3.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC3.pmthresholds.line.nearend.15min.FC	10 (count)
OC3.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC3.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC3.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC3.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC3.pmthresholds.line.nearend.15min.PSC	1 (count)
OC3.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC3.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC3.pmthresholds.line.nearend.15min.UAS	3 (seconds)

Table C-6 OC-3 Card Default Settings (continued)

Property Name	Default Value
OC3.pmthresholds.line.nearend.1day.CV	14120 (B2 count)
OC3.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC3.pmthresholds.line.nearend.1day.FC	40 (count)
OC3.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC3.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC3.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC3.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC3.pmthresholds.line.nearend.1day.PSC	5 (count)
OC3.pmthresholds.line.nearend.1day.PSD	600 (seconds)
OC3.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC3.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC3.pmthresholds.section.nearend.15min.CV	10000 (B1 count)
OC3.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC3.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC3.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC3.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC3.pmthresholds.section.nearend.1day.ES	25 (seconds)
OC3.pmthresholds.section.nearend.1day.SEFS	4095 (seconds)
OC3.pmthresholds.section.nearend.1day.SES	5 (seconds)
OC3.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC3.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC3.pmthresholds.sts.nearend.15min.FC	10 (count)
OC3.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC3.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC3.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC3.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC3.pmthresholds.sts.nearend.1day.FC	10 (count)
OC3.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC3.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-7 lists the default settings for OC-12 cards. The ONS 15454 has four types of OC-12 cards; the default settings are the same for each

Table C-7 OC-12 Card Default Settings

Property Name	Default Value
OC12.config.line.AINSSoakTime	08:00 (hours:mins)
OC12.config.line.EnableSyncMsg	TRUE
OC12.config.line.PJStsMon#	0 (STS #)
OC12.config.line.SDBER	1E-7
OC12.config.line.SFBER	1E-4
OC12.config.line.SendDoNotUse	FALSE
OC12.config.line.State	OOS
OC12.config.sts.IPPMEnabled	FALSE
OC12.pmthresholds.line.farend.15min.CV	5315 (B2 count)
OC12.pmthresholds.line.farend.15min.ES	87 (seconds)
OC12.pmthresholds.line.farend.15min.FC	10 (count)
OC12.pmthresholds.line.farend.15min.SES	1 (seconds)
OC12.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC12.pmthresholds.line.farend.1day.CV	53150 (B2 count)
OC12.pmthresholds.line.farend.1day.ES	864 (seconds)
OC12.pmthresholds.line.farend.1day.FC	40 (count)
OC12.pmthresholds.line.farend.1day.SES	4 (seconds)
OC12.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC12.pmthresholds.line.nearend.15min.CV	5315 (B2 count)
OC12.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC12.pmthresholds.line.nearend.15min.FC	10 (count)
OC12.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC12.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC12.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC12.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC12.pmthresholds.line.nearend.15min.PSC	1 (count)
OC12.pmthresholds.line.nearend.15min.PSC-W	1 (count)
OC12.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC12.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)
OC12.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC12.pmthresholds.line.nearend.15min.UAS	3 (seconds)
OC12.pmthresholds.line.nearend.1day.CV	53150 (B2 count)
OC12.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC12.pmthresholds.line.nearend.1day.FC	40 (count)
OC12.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC12.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)

Table C-7 OC-12 Card Default Settings (continued)

Property Name	Default Value
OC12.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC12.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC12.pmthresholds.line.nearend.1day.PSC	5 (count)
OC12.pmthresholds.line.nearend.1day.PSC-W	5 (count)
OC12.pmthresholds.line.nearend.1day.PSD	600 (seconds)
OC12.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)
OC12.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC12.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC12.pmthresholds.section.nearend.15min.CV	10000 (B1 count)
OC12.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC12.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC12.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC12.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC12.pmthresholds.section.nearend.1day.ES	5000 (seconds)
OC12.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC12.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC12.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC12.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC12.pmthresholds.sts.nearend.15min.FC	10 (count)
OC12.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC12.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC12.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC12.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC12.pmthresholds.sts.nearend.1day.FC	10 (count)
OC12.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC12.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-8 lists the default settings for the OC-48 cards. The ONS 15454 has six types of OC-48 cards; the default settings are the same for each.

Table C-8 OC-48 Default Settings

Property Name	Default Value
OC48.config.line.AINSSoakTime	08:00 (hours:mins)
OC48.config.line.EnableSyncMsg	TRUE
OC48.config.line.PJStsMon#	0 (STS #)
OC48.config.line.SDBER	1E-7
OC48.config.line.SFBER	1E-4
OC48.config.line.SendDoNotUse	FALSE
OC48.config.line.State	OOS
OC48.config.sts.IPPMEnabled	FALSE
OC48.pmthresholds.line.farend.15min.CV	21260 (B2 count)
OC48.pmthresholds.line.farend.15min.ES	87 (seconds)
OC48.pmthresholds.line.farend.15min.FC	10 (count)
OC48.pmthresholds.line.farend.15min.SES	1 (seconds)
OC48.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC48.pmthresholds.line.farend.1day.CV	212600 (B2 count)
OC48.pmthresholds.line.farend.1day.ES	864 (seconds)
OC48.pmthresholds.line.farend.1day.FC	40 (count)
OC48.pmthresholds.line.farend.1day.SES	4 (seconds)
OC48.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC48.pmthresholds.line.nearend.15min.CV	21260 (B2 count)
OC48.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC48.pmthresholds.line.nearend.15min.FC	10 (count)
OC48.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC48.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC48.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC48.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC48.pmthresholds.line.nearend.15min.PSC	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-R	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-S	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-W	1 (count)
OC48.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-R	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-S	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)
OC48.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC48.pmthresholds.line.nearend.15min.UAS	3 (seconds)
OC48.pmthresholds.line.nearend.1day.CV	212600 (B2 count)

Table C-8 OC-48 Default Settings (continued)

Property Name	Default Value
OC48.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC48.pmthresholds.line.nearend.1day.FC	40 (count)
OC48.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC48.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC48.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC48.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC48.pmthresholds.line.nearend.15min.PSC	5 (count)
OC48.pmthresholds.line.nearend.15min.PSC-R	5 (count)
OC48.pmthresholds.line.nearend.15min.PSC-S	5 (count)
OC48.pmthresholds.line.nearend.15min.PSC-W	5 (count)
OC48.pmthresholds.line.nearend.15min.PSD	600 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-R	600 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-S	600 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-W	600 (seconds)
OC48.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC48.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC48.pmthresholds.section.nearend.15min.CV	10000 (B1 count)
OC48.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC48.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC48.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC48.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC48.pmthresholds.section.nearend.1day.ES	500 (seconds)
OC48.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC48.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC48.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC48.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC48.pmthresholds.sts.nearend.15min.FC	10 (count)
OC48.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC48.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC48.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC48.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC48.pmthresholds.sts.nearend.1day.FC	10 (count)
OC48.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC48.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-9 lists the default settings for the OC-192 card.

Table C-9 OC-192 Card Default Settings

Property Name	Default Value
OC192.config.line.AINSSoakTime	08:00 (hours:mins)
OC192.config.line.EnableSyncMsg	TRUE
OC192.config.line.PJStsMon#	0 (STS #)
OC192.config.line.SDBER	1E-7
OC192.config.line.SFBER	1E-4
OC192.config.line.SendDoNotUse	FALSE
OC192.config.line.State	OOS
OC192.config.sts.IPPMEnabled	FALSE
OC192.pmthresholds.line.farend.15min.CV	85040 (B2 count)
OC192.pmthresholds.line.farend.15min.ES	87 (seconds)
OC192.pmthresholds.line.farend.15min.FC	10 (count)
OC192.pmthresholds.line.farend.15min.SES	1 (seconds)
OC192.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC192.pmthresholds.line.farend.1day.CV	850400 (B2 count)
OC192.pmthresholds.line.farend.1day.ES	864 (seconds)
OC192.pmthresholds.line.farend.1day.FC	40 (count)
OC192.pmthresholds.line.farend.1day.SES	4 (seconds)
OC192.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC192.pmthresholds.line.nearend.15min.CV	85040 (B2 count)
OC192.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC192.pmthresholds.line.nearend.15min.FC	10 (count)
OC192.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC192.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC192.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC192.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC192.pmthresholds.line.nearend.15min.PSC	1 (count)
OC192.pmthresholds.line.nearend.15min.PSC-R	1 (count)
OC192.pmthresholds.line.nearend.15min.PSC-S	1 (count)
OC192.pmthresholds.line.nearend.15min.PSC-W	1 (count)
OC192.pmthresholds.line.nearend.15min.PSD	300 (count)
OC192.pmthresholds.line.nearend.15min.PSD-R	300 (count)
OC192.pmthresholds.line.nearend.15min.PSD-S	300 (seconds)
OC192.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)
OC192.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC192.pmthresholds.line.nearend.15min.UAS	3 (seconds)
OC192.pmthresholds.line.nearend.1day.CV	850400 (seconds)

Table C-9 OC-192 Card Default Settings (continued)

Property Name	Default Value
OC192.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC192.pmthresholds.line.nearend.1day.FC	40 (B2 count)
OC192.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (seconds)
OC192.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC192.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC192.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC192.pmthresholds.line.nearend.1day.PSC	5 (count)
OC192.pmthresholds.line.nearend.1day.PSC-R	5 (count)
OC192.pmthresholds.line.nearend.1day.PSC-S	5 (count)
OC192.pmthresholds.line.nearend.1day.PSC-W	5 (count)
OC192.pmthresholds.line.nearend.1day.PSD	600 (count)
OC192.pmthresholds.line.nearend.1day.PSD-R	600 (count)
OC192.pmthresholds.line.nearend.1day.PSD-S	600 (count)
OC192.pmthresholds.line.nearend.1day.PSD-W	600 (count)
OC192.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC192.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC192.pmthresholds.section.nearend.15min.CV	10000 (seconds)
OC192.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC192.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC192.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC192.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC192.pmthresholds.section.nearend.1day.ES	5000 (seconds)
OC192.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC192.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC192.pmthresholds.sts.nearend.15min.CV	15 (B1 count)
OC192.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC192.pmthresholds.sts.nearend.15min.FC	10 (seconds)
OC192.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC192.pmthresholds.sts.nearend.15min.UAS	10 (B3 count)
OC192.pmthresholds.sts.nearend.1day.CV	125 (seconds)
OC192.pmthresholds.sts.nearend.1day.ES	100 (count)
OC192.pmthresholds.sts.nearend.1day.FC	10 (seconds)
OC192.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC192.pmthresholds.sts.nearend.1day.UAS	10 (B3 count)

Node Default Settings

The table in this section lists the node-level default settings for the Cisco ONS 15454. Cisco provides the following types of settings pre-provisioned for each ONS 15454 node:

- UPSR reversion settings determine whether or not UPSR circuits are revertive and, if so, what the reversion time is.
- Defaults Description lists the current defaults file on the node.
- BLSR reversion settings determine whether or not BLSR circuits are revertive and, if so, what the reversion time is.
- IIOP Listener Port sets the IIOP listener port number.
- Login warning message warns users at the login screen about the possible legal or contractual ramifications of accessing equipment, systems, or networks without authorization.
- 1+1 protection settings determine whether or not 1+1 protected circuits are revertive and, if so, what the reversion time is.
- Timing settings determine the AIS threshold, coding, and framing for BITS1 and BITS2 timing.

Table C-10 lists the ONS 15454 node default settings.

Table C-10 Node Default Settings

Property Name	Default Value
NODE.circuits.upsr.ReversionTime	5.0 (minutes)
NODE.circuits.upsr.Revertive	FALSE
NODE.general.DefaultsDescription	Factory Defaults
NODE.general.IIOPListenerPort (reboots node)	57790 (port #)
NODE.general.LoginWarningMessage	LoginWarningMessage=<center><B>WARNING </B><center>This system is restricted to authorized users for business purposes. Unauthorized<p>access is a violation of the law. This service may be monitere for administrative<p> and security reasons. By proceding, you consent to this monitoring.
NODE.protection.1+1.BidirectionalSwitching	FALSE
NODE.protection.1+1.ReversionTime	5.0 (minutes)
NODE.protection.1+1.Revertive	FALSE
NODE.protection.blsr.RingReversionTime	5.0 (minutes)
NODE.protection.blsr.RingRevertive	TRUE
NODE.protection.blsr.SpanReversionTime	5.0 (minutes)
NODE.protection.blsr.SpanRevertive	TRUE
NODE.timing.bits-1.AISThreshold	SMC
NODE.timing.bits-1.Coding	B8ZS
NODE.timing.bits-1.Framing	ESF
NODE.timing.bits-1.State	IS
NODE.timing.bits-2.AISThreshold	SMC

Table C-10 Node Default Settings (continued)

Property Name	Default Value
NODE.timing.bits-2.Coding	B8ZS
NODE.timing.bits-2.Framing	ESF
NODE.timing.bits-2.State	IS
NODE.timing.general.Mode	External
NODE.timing.general.QualityOfRES	RES\=DUS
NODE.timing.general.ReversionTime	5.0 (minutes)
NODE.timing.general.Revertive	FALSE
NODE.timing.general.SSMMessageSet	Generation 1

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 *UPSR*.

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.

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. 1. InterExchange Carrier.
2. 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

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. In this manual the term "node" usually refers to an ONS 15454.

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 unidirectional path switched ring (UPSR) 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. 1. Shielded Twisted Pair.
2. 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.*

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.

UPSR

(Unidirectional Path Switched Ring). 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